Chapter 1: Introduction to Information Security

1.1 Understanding information security

1.2 Elements of information Security

- 1.2(a) Confidentiality
- 1.2(b) Availability
- 1.2(c) Integrity
- 1.2(d) Authenticity
- 1.2(e) Non Repudiation

Chapter2: Risk management

2.1 Introduction

2.2 Defining Risks, threats and Vulnerability

2.3 Risk Identification

- 2.3(a) Asset valuation
- 2.3(b) Threat analysis
- 2.3(c) Vulnerability assessment

2.4 Risk Analysis

- 2.4(a) Qualitative Risk Analysis
- 2.4(b) Quantitative Risk Analysis

2.5 Risk Treatment

- 2.5(a) Risk reduction
- 2.5(b) Risk Transfer
- 2.5(c) Risk Avoidance
- 2.5(d) Risk Acceptance

2.6 Identify Threats

- 2.6(a) Adversarial threats
- 2.6(b) Adversarial threats
- 2.6(c) Structural threats
- 2.6(d) Environmental threats
- 2.6 (e) Insider Threat

2.7 Identify Vulnerabilities

- 2.7(a) Vulnerability assessment
- 2.7(b) Types of Vulnerability assessment
- 2.7(c) Vulnerability assessment scoring system
- 2.7(d) Vulnerability assessment Solutions
- 2.7(e) Vulnerability assessment tools
- 2.7(f) Vulnerability assessment Reports

Chapter 3 Hacking Introduction

3.1 What is Hacking

3.1(a) Defining Hacking

3.1(b) Hacking Concepts

3.2 Types of hackers

3.2(a) Black Hat

3.2(b) White Hat

3.2(c) Grey Hat

3.2(d) Script Kiddies

3.2(e) Hacktivist

3.2(f) Cyber Terrorist

3.2(g) Competitors

3.2(h) State Sponsored

Chapter 4 Malware Threats

4.1 Introduction to MALWARES

4.2 Types of MALWARES

4.2(a) VIRUS

4.2(b) TROJAN

4.2(c) WORMS

4.2(d) ROOT KITS

4.2(e) SPYWARE

4.2(f) RANSOMEWARE

4.2(g) KEYLOGGERS

4.2(h) BOTS

4.2(I) ADWARES

4.2(j) HOAX

4.3 Malware Components

4.3(a) Crypter

4.3(b) Downloader

4.3(c) Injector

4.3(d) Dropper

4.3(e) Exploit

4.3(f) Payload

4.3(g) Obfuscator

4.3(h) Packer

Chapter 5 Network attacks

5.10 DDOS attacks

5.11 Hijacking Attacks

5.11(a) Click jacking

5.11(b) DNS hijacking

5.11(c) Domain hijacking

5.11(d) Session hijacking

5.11(e) URL hijacking/Typosquatting

5.12 Amplification Attack

5.12(a) ICMP amplification

5.12(b) DNS amplification

5.12(c) UDP amplification

5.12(d) NTP amplification

5.13 Pass the Hash Attack

Chapter 6 : Cryptography

6.1 Defining Cryptography

6.2 Objectives of Cryptography

6.3 Types Of Cryptography

6.3(a) Symmetric Encryption

CHAPTER 7 : Cyber Security Policies & Employee's Role & Responsibilities

7.1 Defining cyber security policies

7.1(a) Security Policy Components

- Policy
- Standards
- Guidelines
- Procedures

7.1(b) Common Security Policy Types

- Acceptable Use Policy
- Privacy policy
- Audit policy
- Password policy
- Wireless standards policy
- Social media policy

7.2 Personnel Management

7.2(a) Separation of Duties:

7.2(b) Job Rotations:

7.2(c) Mandatory vacations:

7.3 Employee's Role & Responsibilities

7.3(a) Defining employees roles and responsibilities

7.3(b) 5key thing to pay attention on:

- Software
- Password Practices
- Backups

- Spam And Phishing Education
- Ongoing Updates

7.4 Laws and Regulations governing Cyber security

7.4(a) SOX

7.4(b) HIPPA

7.4(c) PCI-DSS

7.4(d) FISMA

7.4(e) GLBA

7.4(f) GDPR

7.4(g) Data Protection Act

Chapter 8: Social Engineering

8.1 Introduction to Social Engineering

8.2 Basic Components of Social Engineering Attacks

8.2(a) Target Evaluation

8.2(b) Pre-texting

8.2(c) Psychological Manipulation

8.2(d) Building Relationships

8.2(e) Motivation

8.3 Motivation Techniques

- 8.3(a) Authority
- 8.3(b) Scarcity
- 8.3(c) Urgency
- 8.3(d) Social Proof
- 8.3(e) Likeness
- 8.3(f) Fear

8.4 Phishing

- 8.4(a) Smishing
- 8.4(b) Vishing
- 8.4(c) Pharming
- 8.4(d) Spear Phishing
- 8.4(e) Whaling

8.5 Impersonation

8.6 Elicitation

8.7 Baiting

8.8 URL Hijacking/Typo squatting

8.9 Spam/Spim

8.10 Piggybacking

8.11 Tailgating

8.12 Shoulder Surfing

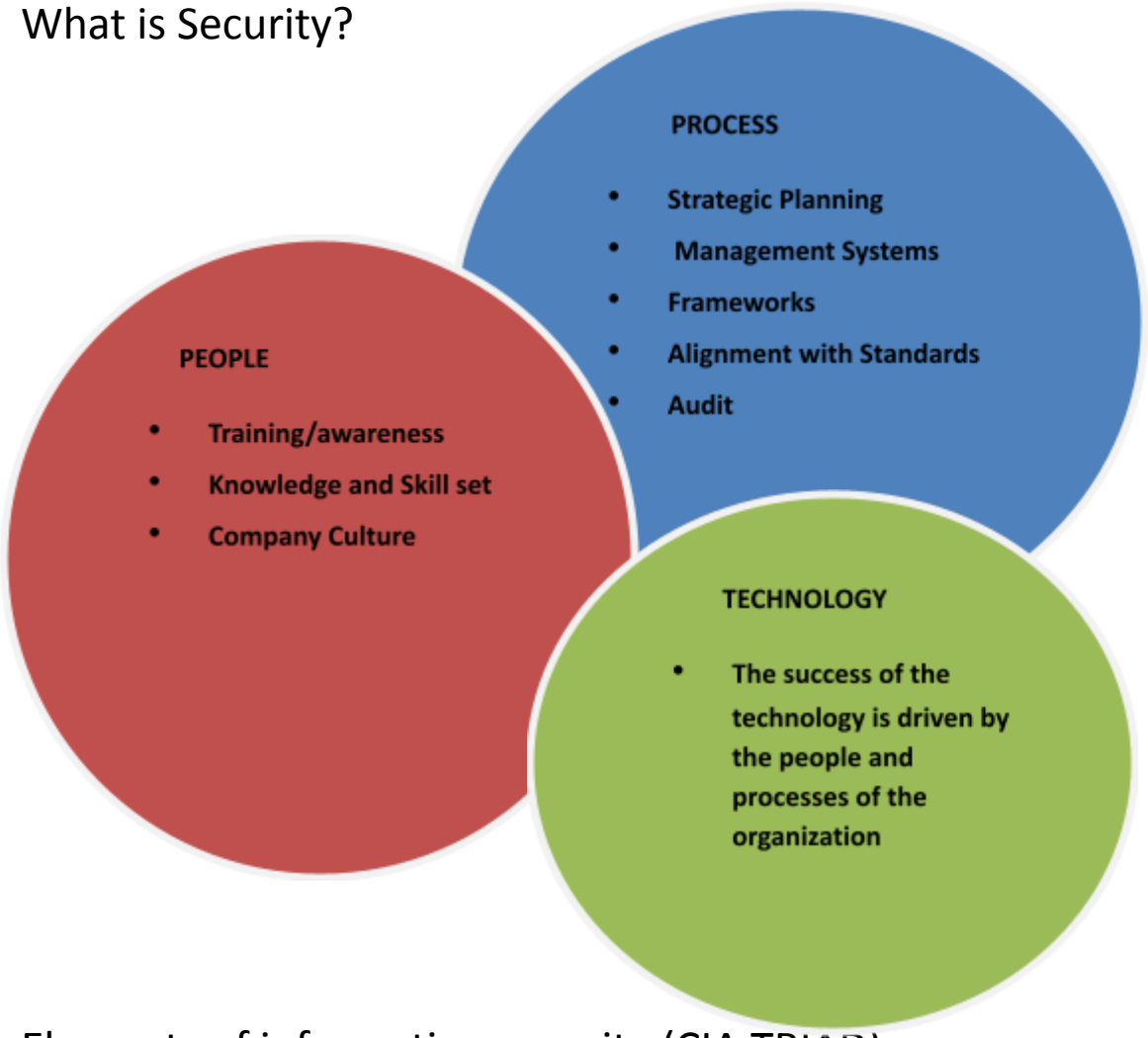
Chapter 1 : Introduction to information Security

Information Security: A managed, risk-based approach to protecting the assets of an organization through applying controls relating to

- People/Human
- Processes/Organizational

- Technology/Technical

What is Security?



Elements of information security (CIA TRIAD)

- **Confidentiality :** Ensures that sensitive information are accessed only by an authorized person and kept away from those not authorized to possess them. It is implemented using security mechanisms such as usernames, passwords, access control lists (ACLs), and encryption.

  Common Attacks Against Confidentiality

- Social engineering
- Monitoring and eavesdropping
- Protocol analyzer (sniffer)
- Espionage
- Theft and burglary

- **Integrity:** Ensures that information are in a format that is true and correct to its original purposes. The receiver of the information must have the information the creator intended him to have. The information can be edited by authorized persons only and remains in its original state when at rest. Integrity is implemented using security mechanism such as data encryption and hashing.

  Common Attacks Against Integrity

  - Malicious code and software
  - System changes
  - Software bugs
  - Data changes and modifications

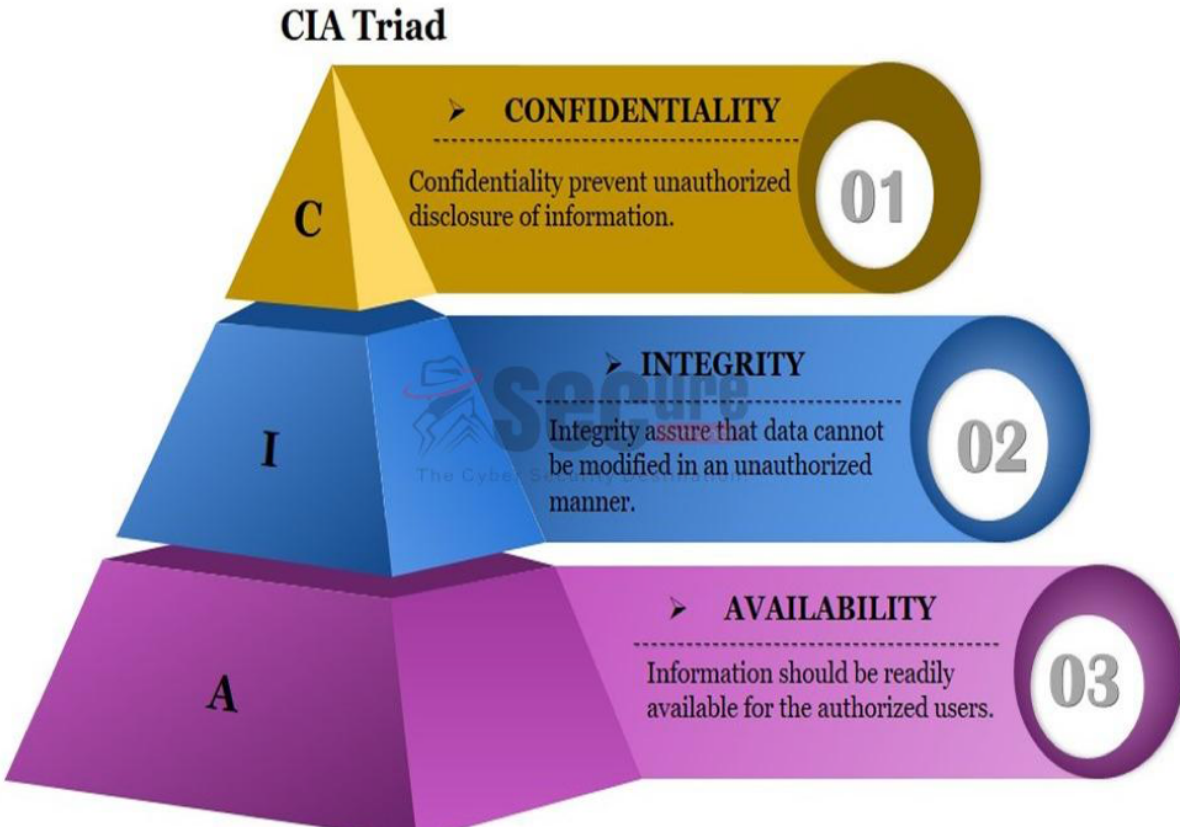
- **Availability:** Ensures that information and resources are available to those who need them. It is implemented using methods such as hardware

maintenance, software patching and network optimization.

Common Attacks Against Availability

- Denial of Service (DoS) or (DDoS) attacks
- Software flaws
- Physical attacks against a facility or system
- Natural disasters

- Authenticity: Authenticity refers to the characteristics of communication, document or any data that ensures the quality of being genuine.
- Non-Repudiation: Guarantee that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message.



The Elements of Information Security:

NIST SP 800-12

- Information security supports the mission of the organization
- Information security is an integral element of sound management

- Information security protections are implemented so as to be commensurate with risk
- Information security roles and responsibilities are made explicit
- Information security responsibilities for system owners go beyond their own organization
- Information security requires a comprehensive an integrated approach
    - Interdependencies of security controls
    - Other interdependencies Information security is assessed and monitored regularly
- Information security is constrained by societal and cultural factors

Information Security Strategy

- A road map--Provides the starting point for the security program
- Long term perspective to help move the organization from current state to desired state (gap analysis)
- Standard across the organization
- Aligned with business strategy/direction

- Understands the culture of the organization
- Reflects business needs and priorities

Chapter 2: Risk Management

Information Security Risk Management : Information security risk management, or ISRM, is the process of managing risks associated with the use of information technology. It involves identifying, assessing, and treating risks to the confidentiality, integrity, and availability of an organization's assets.

Risk Definitions :

- Asset: Anything of Value to the company
- Vulnerability: A weakness; the absence of a safeguard
- Threat: Something that could pose loss to all or part of an asset
- Threat Agent: What carries out the attack
- Exploit: An instance of compromise
- Risk: risk is the concept that indicates exposure to the chances of damage

Risk = Threat × Vulnerability

- Controls: Physical, Administrative, and Technical Protections
    - ❖ Safeguards
    - ❖ Countermeasure
- Total Risk: The risk that exists before any control is implemented
- Residual Risk: Leftover risk after applying a control
- Secondary Risk: When one risk response triggers another risk event

Risk Management Life Cycle:

Risk Management life cycle Steps

- Risk Identification
  - ❖ Asset valuation
  - ❖ Threat analysis
  - ❖ Vulnerability assessment
- Risk Analysis
  - ❖ Qualitative Risk Analysis
  - ❖ Quantitative Risk Analysis
- Risk Treatment

- ❖ Risk reduction
- ❖ Risk Transfer
- ❖ Risk Avoidance
- ❖ Risk Acceptance

Risk Identification

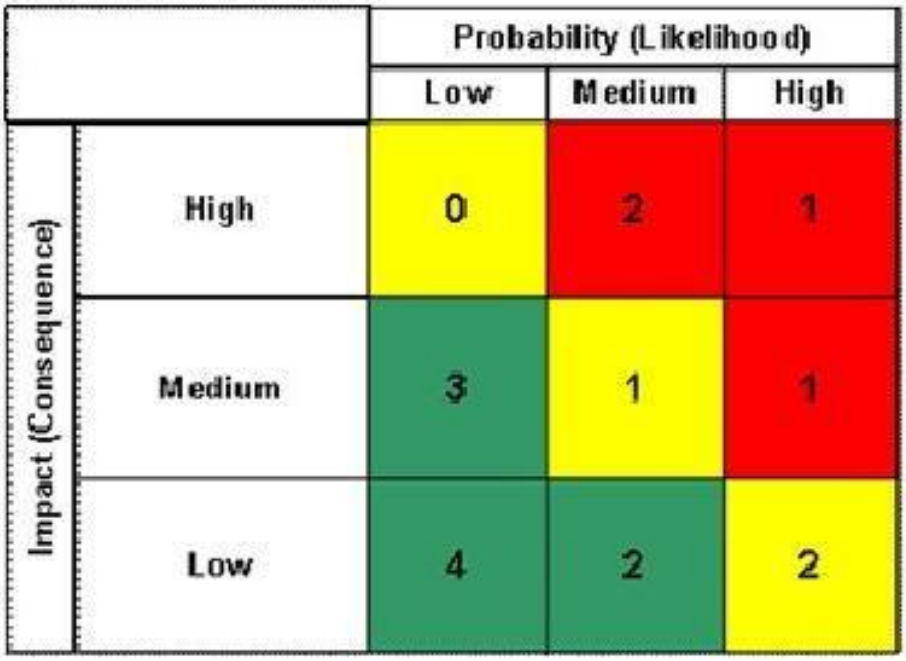
- Asset valuation
  - ❖ Identifying an organization's assets and determining their value is a critical step in determining the appropriate level of security
- Threat analysis
  - ❖ Define the actual threat
  - ❖ Identify possible consequences to the organization if the threat event occurs.
  - ❖ Determine the probable frequency of a threat event.
  - ❖ Assess the probability that a threat will actually materialize
- Vulnerability assessment
  - ❖ A vulnerability assessment provides a valuable baseline for determining appropriate and necessary safeguards.

Risk Analysis

- Methodical examination that brings together all the elements of risk management (identification, analysis, and

control) and is critical to an organization for developing an effective risk management strategy

- A risk analysis involves the following four steps:
  - ❖ Identify the assets to be protected, including their relative value, sensitivity, or importance to the organization
  - ❖ Define specific threats, including threat frequency and impact data.
  - ❖ Calculate Annualized Loss Expectancy (ALE).
  - ❖ Select appropriate safeguards.
- **Qualitative**
  - ❖ Subjective analysis to help prioritize probability and impact of risk events.
  - ❖ Assess risks based on subjective input
  - ❖ Uses terms like high, medium, low
  - ❖ Inexpensive, and quick way to begin the prioritization and ranking of risks



		Probability (Likelihood)		
		Low	Medium	High
Impact (Consequence)	High	0	2	1
	Medium	3	1	1
	Low	4	2	2

Qualitative assessment

- **Quantitative**
  - ❖ Providing a dollar value to a particular risk event.
  - ❖ Much more sophisticated in nature, a quantitative analysis if much more difficult and requires a special skill set
  - ❖ Business decisions are made on a quantitative analysis
  - ❖ Can't exist on its own. Quantitative analysis depends on qualitative information
  - ❖ More experience required than with Qualitative
  - ❖ Involves calculations to determine a dollar value associated with each risk event
  - ❖ Business Decisions are made on this type of analysis
  - ❖ Goal is to the dollar value of a risk and use that amount to determine what the best control is for a particular asset
  - ❖ Necessary for a cost/benefit analysis

Quantitative Analysis Formulas and Terms

- (**AV) Asset Value**: Dollar figure that represents what the asset is worth to the organization

- **(EF) Exposure Factor**: The percentage of loss that is expected to result in the manifestation of a particular risk event.
- **(SLE) Single Loss Expectancy**: Dollar figure that represents the cost of a single occurrence of a threat instance
- **(ARO) Annual Rate of Occurrence**: How often the threat is expected to materialize
- **(ALE) Annual Loss Expectancy**: Cost per year as a result of the threat
- **(TCO) Total Cost of Ownership** is the total cost of implementing a safeguard. Often in addition to initial costs, there are ongoing maintenance fees as well.
- **(ROI) Return on Investment:** Amount of money saved by implementation of a safeguard. Sometimes referred to as the value of the safeguard/control.

Where :

SLE = AV * EF

ALE = SLE * ARO

TCO = Initial Cost of Control + Yearly fees

ROI= Return on Investment:

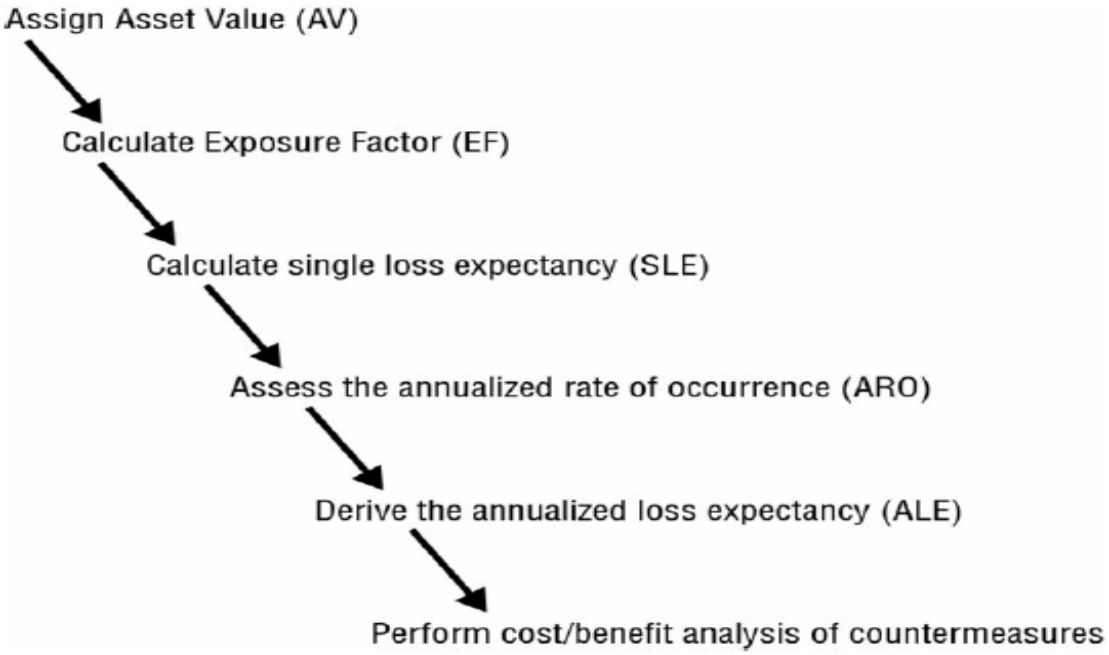
ALE (before implementing control)

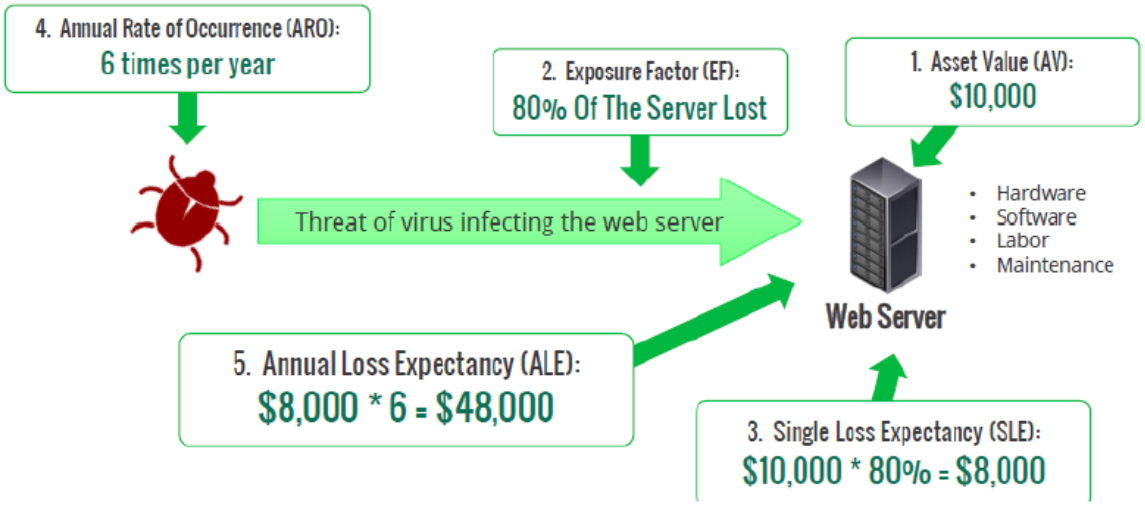
– ALE (after implementing control)

– cost of control

= ROI (Value of Control)

Steps for Quantitative Analysis





Quantitative Assessment

Risk Treatment /Response

Risk Avoidance	Risk Transference
Risk Mitigation	Risk acceptance

Risk Avoidance/Reduction

- Risk reduction means that action is taken to lessen the frequency and/or impact of a risk.
  - May require the use of several controls until it reaches levels of risk acceptance or risk tolerance
- Examples of risk mitigation:
  - Strengthening overall risk management practices, such as implementing sufficiently mature risk management processes
  - Deploying new technical, management or operational controls that reduce either the likelihood or the impact of an adverse event
  - Installing a new access control system
  - Implementing policies or operational procedures
  - Developing an effective incident response and business continuity plan (BCP)
  - Using compensating controls

****The ultimate risk reduction is avoidance**

Risk Transference

- ❖ Risk transference is a decision to reduce loss through sharing that risk with another organization
- ❖ SLAs (Service Level Agreements) and contracts establish the degree of transference

Risk Acceptance

- ❖ The practice of accepting certain risk(s) based on a business decision that weighs the cost versus the benefit of a risk

Examples of risk acceptance:

- Provides no active mitigation
- Based on a cost/benefit analysis, it is determined the cost of the control is less than the potential for loss
- Sometimes acceptance is the only choice.
- Risk acceptance still includes due diligence, and can still be used to indicate good business decisions were made
- Level of risk and impact is always changing, so regular reviews are needed

Risk Mitigation

- The decrease in the level of risk presented through implementation of controls

Identify Threats

Threats: A threat in the world of cyber security is an outside force that may exploit vulnerability.
For example, a hacker who would like to conduct a DoS attack against a website and knows about an Apache vulnerability poses a clear cyber security threat. Although many threats are malicious in nature, this is not necessarily the case. For example, an earthquake may also disrupt the availability of a website by damaging the datacenter containing the web servers. Earthquakes clearly do not have malicious intent. In most cases, cyber security professionals

cannot do much to eliminate a threat. Hackers will hack and earthquakes will strike whether we like it or not.

NIST identifies four different categories of threats that an organization might face and should consider in its threat identification process:

Adversarial threats: are individuals, groups, and organizations that are attempting to deliberately undermine the security of an organization.Adversaries may include trusted insiders, competitors, suppliers,customers, business partners, or even nation-states. When evaluating an adversarial threat, cybersecurity analysts should consider the capability of the threat actor to engage in attacks, the intent of the threat actor, and the likelihood that the threat will target the organization.

Accidental threats occur when individuals doing their routine work mistakenly perform an action that undermines security. For example, a system administrator might accidentally delete a critical disk volume, causing a loss of availability. When evaluating an accidental threat, cybersecurity analysts should consider the possible range of effects that the threat might have on the organization.

Structural threats occur when equipment, software, or environmental controls fail due to the exhaustion of resources (such as running out of gas), exceeding their operational capability (such as operating in extreme heat), or simply failing due to age. Structural threats may come from

IT components (such as storage, servers, and network devices), environmental controls (such as power and cooling infrastructure), and software (such as operating systems and applications). When evaluating a structural threat, cybersecurity analysts should consider the possible range of effects that the threat might have on the organization.

Environmental threats occur when natural or man-made disasters occur that are outside the control of the organization. These might include fires, flooding, severe storms, power failures, or widespread telecommunications disruptions. When evaluating a structural threat, cybersecurity analysts should consider the possible range of effects that the threat might have on the organization.

Insider Threat : When performing a threat analysis, cybersecurity professionals must remember that threats come from both external and internal sources. In addition to the hackers, natural disasters, and other threats that begin outside the organization, rouge employees, disgruntled team members, and incompetent administrators also pose a significant threat to enterprise cybersecurity. As an organization designs controls, it must consider both internal and external threats.

Identify Vulnerabilities

Vulnerability: A vulnerability is a weakness in a device, system, application, or process that might allow an attack to take place. Vulnerabilities are internal factors that may be controlled by cybersecurity professionals. For example, a web server that is running an outdated version of the Apache service may contain a vulnerability that would allow an attacker to conduct a denial-of-service (DoS) attack against the websites hosted on that server, jeopardizing their availability. Cybersecurity professionals within the organization have the ability to remediate this vulnerability by upgrading the Apache service to the most recent version that is not susceptible to the DoS attack.

Vulnerbility assessment: A vulnerability assessment provides an organization with information on the security weaknesses in its environment and provides direction on how to assess the risks associated with those weaknesses and evolving threats. This process offers the organization a better understanding of its assets, security flaws and overall risk, reducing the likelihood that a cybercriminal will breach its systems and catch the business off guard.

Types of vulnerability assessments

Vulnerability assessments depend on discovering different types of system or network vulnerabilities, which means the assessment process includes using a variety of tools, scanners and methodologies to identify vulnerabilities, threats and risks.

Some of the different types of vulnerability assessment scans include the following:

- Network-based scans are used to identify possible network security attacks. This type of scan can also detect vulnerable systems on wired or wireless networks.
- Host-based scans are used to locate and identify vulnerabilities in servers, workstations or other network hosts. This type of scan usually examines ports and services that may also be visible to network-based scans, but it offers greater visibility into the configuration settings and patch history of scanned systems.
- Wireless network scans of an organization's Wi-Fi networks usually focus on points of attack in the wireless network infrastructure. In addition to identifying rogue access points, a wireless network scan can also validate that a company's network is securely configured.

- Application scans can be used to test websites in order to detect known software vulnerabilities and erroneous configurations in network or web applications.
- Database scans can be used to identify the weak points in a database so as to prevent malicious attacks, such as SQL injection attacks.

Vulnerability assessment Scoring system

The Common Vulnerability Scoring System (CVSS) provides a way to capture the principal characteristics of a vulnerability and produce a numerical score reflecting its severity. The numerical score can then be translated into a qualitative representation (such as low, medium, high, and critical) to help organizations properly assess and prioritize their vulnerability management processes.

Analysts scoring a new vulnerability begin by rating the vulnerability on six different measures. Each measure is given both a descriptive rating and a numeric score.

- **Access Vector Metric**
- **Access Complexity Metric**
- **Authentication Metric**
- **Confidentiality Metric**
- **Integrity Metric**

❖ Availability Metric

Access Vector Metric : The access vector metric describes how an attacker would exploit the vulnerability and is assigned according to the following table.

Value	Description	Score
Local (L)	The attacker must have physical or logical access to the affected system.	0.395
Adjacent Network (A)	The attacker must have access to the local network that the affected system is connected to.	0.646
Network (N)	The attacker can exploit the vulnerability remotely over a network.	1.000

Access Complexity Metric: The *access complexity metric* describes the difficulty of exploiting the vulnerability and is assigned according to the following table.

Value	Description	Score
High (H)	Exploiting the vulnerability requires "specialized" conditions that would be difficult to find.	0.350
Medium (M)	Exploiting the vulnerability requires "somewhat specialized" conditions.	0.610
Low (L)	Exploiting the vulnerability does not require any specialized conditions.	0.710

Authentication Metric: The authentication metric describes the authentication hurdles that an attacker would need to clear to exploit a vulnerability and is assigned according to the following table.

Value	Description	Score
Multiple (M)	Attackers would need to authenticate two or more times to exploit the vulnerability.	0.450
Single (S)	Attackers would need to authenticate once to exploit the vulnerability.	0.560
None (N)	Attackers do not need to authenticate to exploit the	0.704

	vulnerability.	

Confidentiality Metric : The confidentiality metric describes the type of information disclosure that might occur if an attacker successfully exploits the vulnerability. The confidentiality metric is assigned according the

Value	**Description**	**Score**
None (N)	There is no confidentiality impact.	0.000
Partial (P)	Access to some information is possible, but the attacker does not have control over what information is compromised.	0.275
Complete (C)	All information on the system is compromised.	0.660

Integrity Metric: The integrity metric describes the type of information alteration that might occur if an attacker successfully exploits the vulnerability. The integrity metric is assigned according to the following table.

Value	Description	Score
None (N)	There is no integrity impact.	0.000
Partial (P)	Modification of some information is possible, but the attacker does not have control over what information is modified.	0.275
Complete (C)	The integrity of the system is totally compromised, and the attacker may change any information at will.	0.660

Availability Metric: The availability metric describes the type of disruption that might occur if an attacker successfully exploits the vulnerability. The availability metric is assigned according to the following table.

Value	**Description**	**Score**
None (N)	There is no availability impact.	0.000
Partial (P)	The performance of the system is degraded.	0.275
Complete (C)	The system is completely shut down.	0.660

Interpreting the CVSS Vector: The CVSS vector uses a single-line format to convey the ratings of a vulnerability on all six of the metrics described in the preceding sections. For Example.

CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N

This vector contains seven components. The first section, "CVSS2#," simply informs the reader (human or system) that the vector was composed using CVSS version 2. The next six sections correspond to each of the six CVSS metrics. In this case, the SSH cipher vulnerability received the following ratings:

Access Vector: Network (score: 1.000)
Access Complexity: Medium (score: 0.610)
Authentication: None (score: 0.704)
Confidentiality: Partial (score: 0.275)
Integrity: None (score: 0.000)
Availability: None (score: 0.000)

**The CVSS vector provides good detailed information on the nature of the risk posed by a vulnerability, but the complexity of the vector makes it difficult to use in prioritization exercises. For this reason, analysts can calculate the *CVSS base score*, which is a single number

representing the overall risk posed by the vulnerability. Arriving at the base score requires first calculating the

- **exploitability score**
- **Impact score**
- **Impact function.**

Calculating the Exploitability Score

Analysts may calculate the exploitability score for a vulnerability using thisformula:

Exploitability = 20 × AccessVector × AccessComplexity × Authentication

Plugging in values for our SSH vulnerability, we get

Exploitability = 20 × 1.000 × 0.610 × 0.704

Exploitability = 8.589

Calculating the Impact Score

Analysts may calculate the impact score for a vulnerability using this formula:

Impact = 10.41 × (1 − (1 − Confidentiality) × (1 − Integrity) × (1 −Availability))

Plugging in values for our SSH vulnerability, we get

Impact = 10.41 × (1 − (1 − 0.275) × (1 − 0) × (1 − 0))

Impact = 10.41 × (1 − (0.725) × (1) × (1))

Impact = 10.41 × (1 − 0.725)

Impact =10.41 × 0.275

Impact = 2.863

Determining the Impact Function Value

The impact function is a simple check. If the impact score is 0, the impact function value is also 0. Otherwise, the impact function value is 1.176. So, in our example case:

ImpactFunction = 1.176

Calculating the Base Score

With all of this information at hand, we can now calculate the CVSS base

score using this formula:

BaseScore = ((0.6 × Impact) + (0.4 × Exploitability) − 1.5) × ImpactFunction

Plugging in values for our SSH vulnerability, we get

BaseScore = ((0.6 × 2.863) + (0.4 × 8.589) − 1.5) × 1.176

BaseScore = (1.718 + 3.436 − 1.5) × 1.176

BaseScore = 3.654 × 1.176

BaseScore = 4.297

Categorizing CVSS Base Scores: Many vulnerability scanning systems further summarize CVSS results by using risk categories, rather than numeric risk ratings.

CVSS score	Risk category
Under 4.0	Low
4.0 or higher, but less than 6.0	Medium
6.0 or higher, but less than 10.0	High
10.0	Critical

Vulnerability assessment tools examples

- Qualys guard: s a popular SaaS (software as a service) vulnerability management offering. It's web-based UI offers network discovery and mapping, asset prioritization, vulnerability assessment reporting and remediation tracking according to business ris
- Nessus: Nessus is capable of scanning the vulnerabilities which allow remote hacking of sensitive data from a system
- Nikto: Nikto is a free software command-line vulnerability scanner that scans webservers for dangerous files/CGIs, outdated server software and other problems.

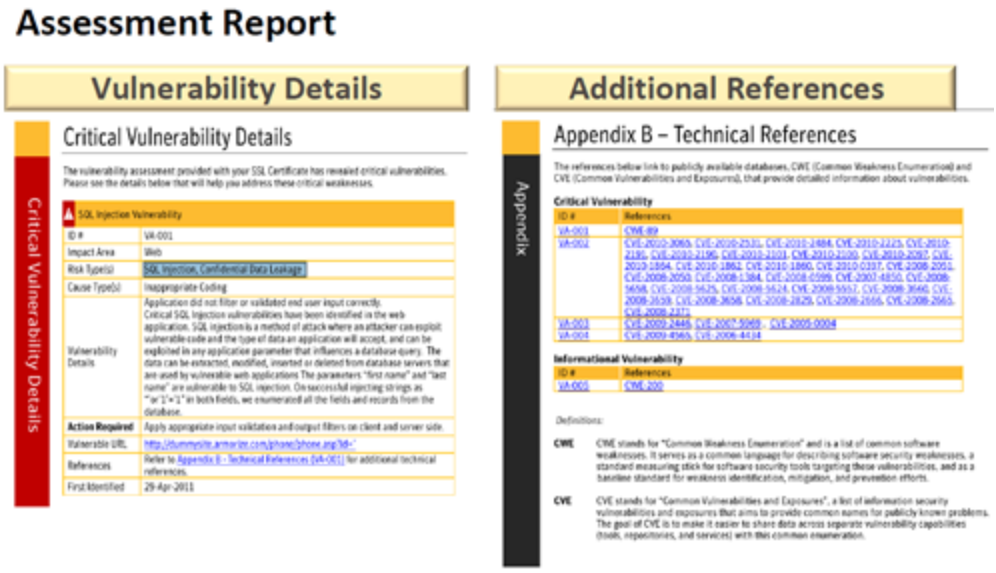
- OpenVAS: From the name itself, we can come to the conclusion that this tool is an open source tool. OpenVAS serves as a central service that provides tools for both vulnerability scanning and vulnerability management.

- Netsparker : is a dead accurate automated scanner that will identify vulnerabilities such as SQL Injection and Cross-site Scripting in web applications and web APIs
- Acunetix: is a fully automated web vulnerability scanner that detects and reports on over 4500 web application vulnerabilities including all variants of SQL Injection and XSS.
- Intruder: is a proactive vulnerability scanner that scans you as soon as new vulnerabilities are released. In addition, it has over 10,000 historic security checks, including for WannaCry, Heartbleed and SQL Injection
- Probely: scans your Web Applications to find vulnerabilities or security issues and provides guidance on how to fix them, having Developers in mind.
- Nexpose Community: Nexpose vulnerability scanner which is an open source tool is developed by Rapid7 is used to scan the vulnerabilities and perform various network checks.

Vulnerability assessment Reports

- Vulnerability assessment Reports discloses the risk detected after scanning the network

- ❖ The Report Alerts the organization of possible attacks and suggest countermeasures
- ❖ Information Available in the report is used to fix security flaws.



Assessment Report

Vulnerability Details

Critical Vulnerability Details

Critical Vulnerability Details

The vulnerability assessment provided with your SSL Certificate has revealed critical vulnerabilities. Please see the details below that will help you address these critical weaknesses.

SQL Injection Vulnerability	
ID #	VA-001
Impact Area	Web
Risk Type(s)	SQL Injection, Confidential Data Leakage
Cause Type(s)	Inappropriate Coding
Vulnerability Details	Application did not filter or validated end user input correctly. Critical SQL Injection vulnerabilities have been identified in the web application. SQL Injection is a method of attack where an attacker can exploit vulnerable code and the type of data an application will accept, and can be exploited in any application parameter that influences a database query. The data can be extracted, modified, inserted or deleted from database servers that are used by vulnerable web applications The parameters "first name" and "last name" are vulnerable to SQL injection. On successful injecting strings as "or '1'='1" in both fields, we enumerated all the fields and records from the database.
Action Required	Apply appropriate input validation and output filters on client and server side.
Vulnerable URL	http://dummysite.armorize.com/phone/phone.asp?id='
References	Refer to Appendix B - Technical References [VA-001] for additional technical references.
First Identified	29-Apr-2011

Additional References

Appendix

Appendix B – Technical References

The references below link to publicly available databases, CWE (Common Weakness Enumeration) and CVE (Common Vulnerabilities and Exposures), that provide detailed information about vulnerabilities.

Critical Vulnerability

ID #	References
VA-001	CWE-89
VA-002	CVE-2010-3083, CVE-2010-2531, CVE-2010-2884, CVE-2010-2225, CVE-2010-2135, CVE-2010-2190, CVE-2010-2101, CVE-2010-2100, CVE-2010-2097, CVE-2010-1864, CVE-2010-1862, CVE-2010-1860, CVE-2010-0397, CVE-2008-2051, CVE-2008-2050, CVE-2008-1384, CVE-2008-0599, CVE-2007-4850, CVE-2008-1658, CVE-2008-5625, CVE-2008-5624, CVE-2008-5557, CVE-2008-3646, CVE-2008-3639, CVE-2008-3658, CVE-2008-2829, CVE-2008-2666, CVE-2008-2665, CVE-2008-2237,
VA-003	CVE-2000-2444, CVE-2007-5069 , CVE-2005-0004
VA-004	CVE-2009-4565, CVE-2006-4434

Informational Vulnerability

ID #	References
VA-005	CWE-200

Definitions:

CWE CWE stands for "Common Weakness Enumeration" and is a list of common software weaknesses. It serves as a common language for describing software security weaknesses, a standard measuring stick for software security tools targeting these vulnerabilities, and as a baseline standard for weakness identification, mitigation, and prevention efforts.

CVE CVE stands for "Common Vulnerabilities and Exposures", a list of information security vulnerabilities and exposures that aims to provide common names for publicly known problems. The goal of CVE is to make it easier to share data across separate vulnerability capabilities (tools, repositories, and services) with this common enumeration.

Chapter 3: Hacking Introduction

Hacking: Hacking generally refers to unauthorized intrusion into a computer or a network. The person engaged in hacking activities is known as a hacker. This hacker may alter system or security features to accomplish a goal that differs from the original purpose of the system.

Hackers: A Hacker is a person who finds and exploits the weakness in computer systems and/or networks to gain access. Hackers are usually skilled computer programmers with knowledge of computer security.Hackers are classified according to the intent of their actions.

Types of Hackers

- **(White hat):** A hacker who gains access to systems with a view to fix the identified weaknesses. They may also perform penetrationTesting and vulnerability assessments.
- **Cracker (Black hat):** A hacker who gains unauthorized access to computer systems for personal gain. The intent is usually to steal corporate data, violate privacy rights, transfer funds from bank accounts etc.
- **Grey hat:** A hacker who is in between ethical and black hat hackers. He/she breaks into computer systems

without authority with a view to identify weaknesses and reveal them to the system owner.

- **Script Kiddies:** A non-skilled person who gains access to computer systems using already made tools
- **Hacktivist:** A hacker who use hacking to send social, religious, and political, etc. messages. This is usually done by hijacking websites and leaving the message on the hijacked website.
- **State Sponcerd:** State or Nation sponsored hackers are those who have been employed by their state or nation's government to snoop in and penetrate through full security to gain confidential information from other governments to stay at the top online
- **Cyber Terrorist:** Cyber terrorism is the use of the Internet to conduct violent acts that result in, or threaten, loss of life or significant bodily harm, in order to achieve political or ideological gains through threat or intimidation
- **Competetors:** Organizations that gains unauthorized access to a business rival's sensitive information
- **Malicious Insider:** A malicious insider or a whistleblower may be an employee with a grudge or a strategic employee compromised or hired by rivals to garner trade secrets of their opponents to stay on top of their game.

Chapter 5 : Malware Threats

Malware: short for “malicious software”: hostile applications that are created with the express intent to damage or disable mobile devices, computers or network servers. Malware’s objectives can include disrupting computing or communication operations, stealing sensitive data, accessing private networks, or hijacking systems to exploit their resources.

Types of Malwares

- **Virus:** A virus is malware that attaches to another program and, when executed usually inadvertently by the user replicates itself by modifying other computer programs and infecting them with its own bits of code.
- **Worms** :Worms are type of malware similar to viruses, self-replicating in order to spread to other computers over a network, usually causing harm by destroying data and files.
- **Trojan:** Trojan is one of the most dangerous malware types. It usually represents itself as something useful in order to trick you. Once it’s on your system, the attackers behind the Trojan gain unauthorized access to the affected computer. From there, Trojans can be used

to steal financial information or install threats like viruses and ransomware.

- **Ransomware:** is a form of malware that locks you out of your device and/or encrypts your files, then forces you to pay a ransom to get them back. Ransomware has been called the cyber criminal's weapon of choice because it demands a quick, profitable payment in hard-to-trace cryptocurrency. The code behind ransomware is easy to obtain through online criminal marketplaces and defending against it is very difficult.
- **Adware** is unwanted software designed to throw advertisements up on your screen, most often within a web browser. Typically, it uses an underhanded method to either disguise itself as legitimate, or piggyback on another program to trick you into installing it on your PC, tablet, or mobile device.
- **Spyware** is malware that secretly observes the computer user's activities without permission and reports it to the software's author.
- **Rootkit** is a form of malware that provides the attacker with administrator privileges on the infected system. Typically, it is also designed to stay hidden from the user, other software on the system, and the operating system itself.
- **Keylogger** is malware that records all the user's keystrokes on the keyboard, typically storing the gathered information and sending it to the attacker,

who is seeking sensitive information like usernames, passwords, or credit card details.

- **Hoax**: A virus hoax is a false warning about a computer virus.

Malware Components

- Crypter: It is a type of software that protects malware from analysis
- Downloader: Downloads malware from internet.
- Injector: Program that injects codes into services
- Dropper: Installs malwares into the system
- Exploit: Malicious code that breaches system security
- Payload: Piece of software that controls the system after exploitation
- Obfuscator: Conceals its purpose and is hard to detect
- Packer: Bundle all files in one and bypass the security
- Malicious code: Command that defines malware functions

Malware Analysis: Malware analysis is the study or process of determining the functionality, origin and potential impact of a given malware sample such as a virus, worm, Trojan, root kit.

Types of Malware Analysis

- Static Malware Analysis

- Dynamic Malware analysis

Static Malware Analysis/Code Analysis : Static Analysis also called static code analysis, is a process of software debugging without executing the code or program. In other words, it examines the malware without examining the code or executing the program. The techniques of static malware analysis can be implemented on various representations of a program. The techniques and tools instantaneously discover whether a file is of malicious intent or not. Then the information on its functionality and other technical indicators help create its simple signatures.

Static Malware Analysis Techniques:

- File Finger Printing : It Examines the evident elements of binary code which includes process in document level. This process includes calculation of cryptographic hashes of binary code to recognize its functions & compare it to the binary codes & programs faces in past scenario.
- Local and Online malware scanning: It calculates the hashes of the suspected file & compare it to offline online malware databases.
- Performing String search: Search embedded malicious string.
- Identifying Packing/Obfuscator methods: Identifying packet elements & tools used for packing.
- Finding Portable Executable information: The PE format stores information a windows system requires to manage executable code.PE stores metadata about the

program which helps in finding extra details about the file.

- ❖ Identifying File Dependencies: Any software program depends upon various inbuilt libraries of an operating system that help in performing specific function. These files contains run time requirement of an application.
- ❖ Malware Disassembly: Helps to find the language used for programming the malware

<u>Dynamic Malware Analysis/Behaviour Analysis:</u> The dynamic analysis runs malware to examine its behavior, learn its functionality and recognize technical indicators. When all these details are obtained, they are used in the detection signatures. The technical indicators exposed may comprise of IP addresses, domain names, file path locations, additional files, registry keys, found on the network or computer.

Dynamic Analysis includes 2 things:

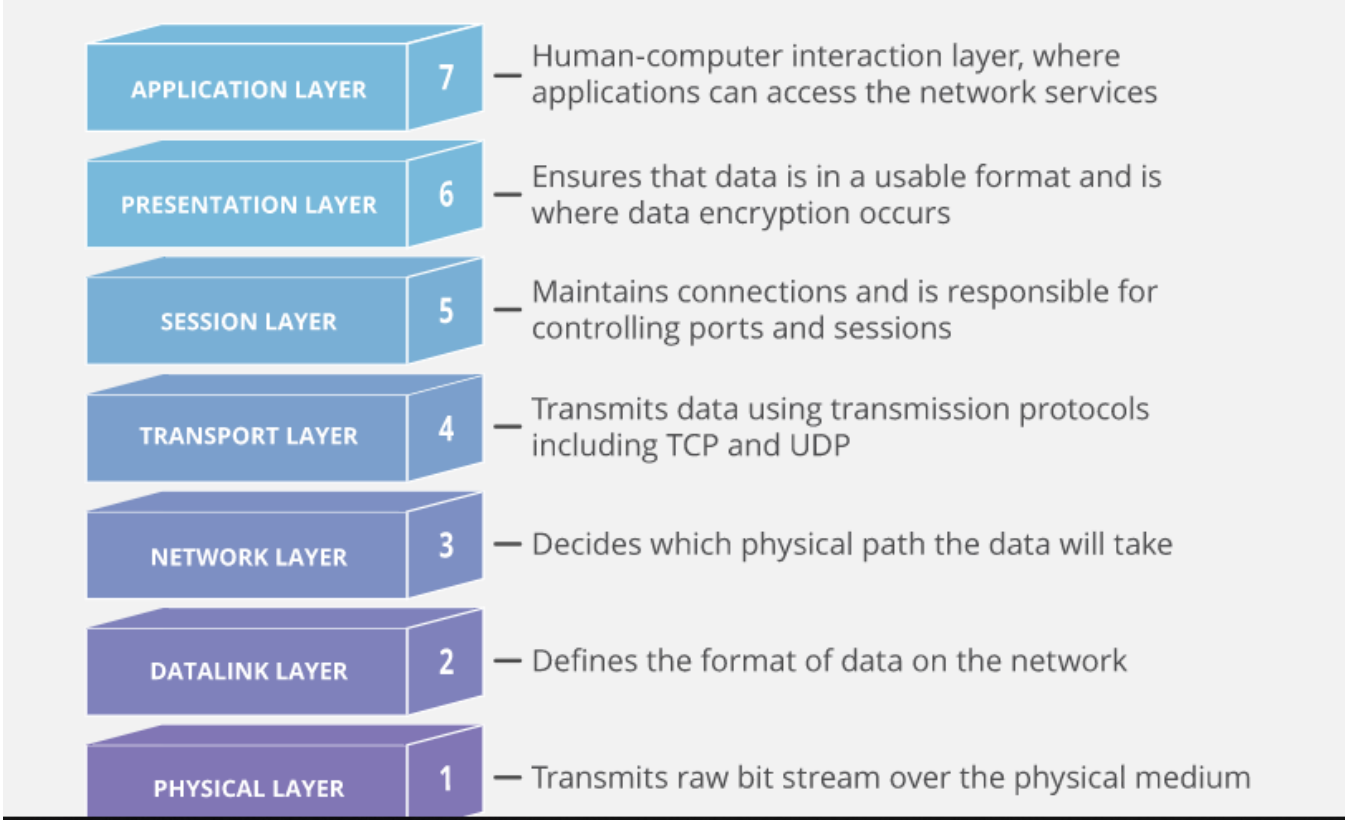
- ❖ **System Baselining :**Refers to taking snapshots of the system at the time malware analysis begins. main purpose of system baselining is to identify significant changes from baseline state. System baselining includes details of registry, file system, open ports, network activity etc.
- ❖ **Host Integrity Monitoring :** It involves taking a snapshot of the system before and after the incident and action using same tools and analyze the changes to evaluate the impact on the system and its properties.

Host Integrity Monitoring includes the following:

- Installation monitor: Helps investigators to find& detect hidden background installation which malware performs.
- Process monitor: To understand the process a malware initiates and takes over after execution.
- Files and Folder monitor: To examine real time file system and folder activity
- Registry monitor :To detect the changes made to the registry by suspicious program
- Network activity monitor :To monitor traffic from & to the victims computer
- Port monitor : To monitor live open port in the infected system and the remote system port numbers requested by the infected system while trying to connect to a email server.
- DNS monitor: To verify DNS servers malware try to connect & to identify type of connections.
- API calls monitor: used to intercept API calls from suspected program to the operating system.
- Device drivers monitor: Scans for suspicious device drivers & verify if they have been downloaded from publishers original site.
- Startup program monitor: Scanning for suspicious programs is essential for detecting Trojan because Trojan & malware alter the system setting & add themselves to the startup menu.

Chapter 6: Network attacks

OSI Model: OSI stands for Open Systems Interconnection. It has been developed by International Organization of Standardization in the year 1974. It is a 7 layer architecture with each layer having specific functionality to perform. All these 7 layers work collaboratively to transmit the data from one person to another across the globe.

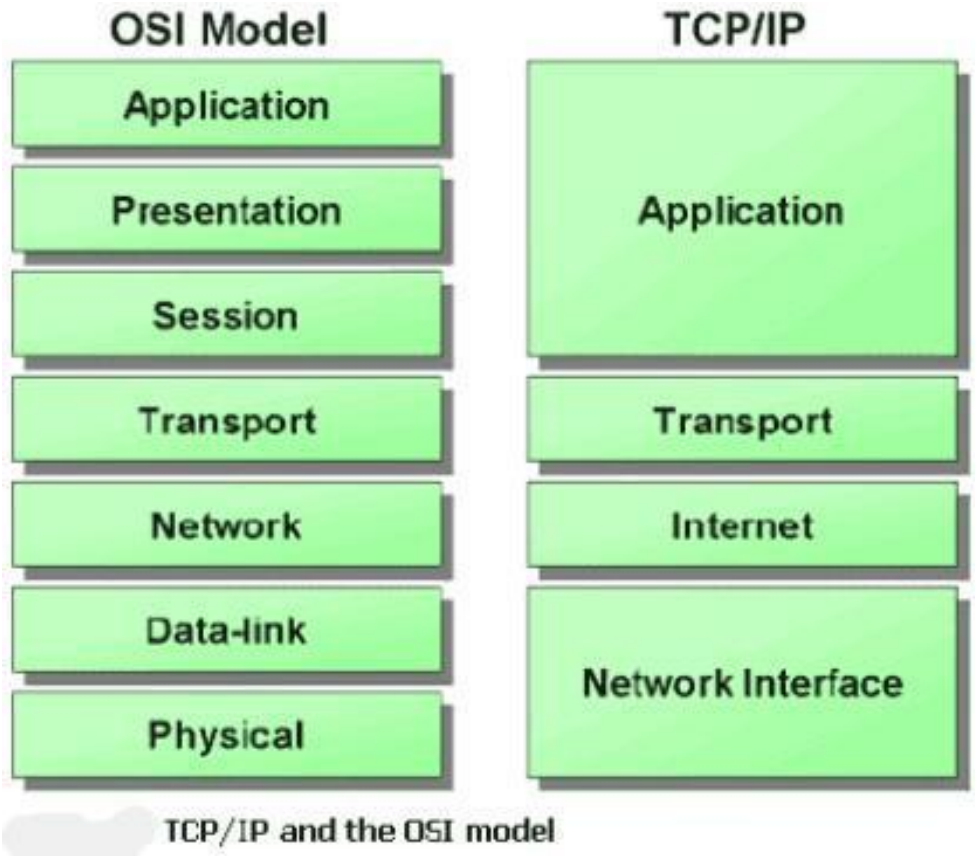


TCP/IP Model : TCP/IP model, it was designed and developed by Department of Defense (DoD) in 1960s and is based on standard protocols. It stands for Transmission Control Protocol/Internet Protocol. The TCP/IP model is a concise version of the OSI model. It contains four layers, unlike seven layers in the OSI model.

The two main protocols in the internet protocol suite serve specific functions.

TCP defines how applications can create channels of communication across a network. It also manages how a message is assembled into smaller packets before they are then transmitted over the internet and reassembled in the right order at the destination address.

IP defines how to address and route each packet to make sure it reaches the right destination. Each gateway computer on the network checks this IP address to determine where to forward the message.



TCP/IP and the OSI model

Spoofing: Spoofing is the act of disguising a communication from an unknown source as being from a known, trusted source. Spoofing can apply to emails, phone calls, and websites, or can be more technical, such as a computer spoofing an IP address, Address Resolution Protocol (ARP), or Domain Name System (DNS) server.

Spoofing Attacks: A spoofing attack is when a malicious party impersonates another device or user on a network in order to launch attacks against network hosts, steal data, spread malware or bypasses access controls. There are

several different types of spoofing attacks that malicious parties can use to accomplish this.

- ❖ IP Address spoofing
- ❖ MAC Address spoofing
- ❖ ARP spoofing
- ❖ DNS spoofing

IP Address Spoofing: In an IP address spoofing attack, an attacker sends IP packets from a false (or "spoofed") source address in order to disguise itself. Denial-of-service attacks often use IP spoofing to overload networks and devices with packets that appear to be from legitimate source IP addresses.

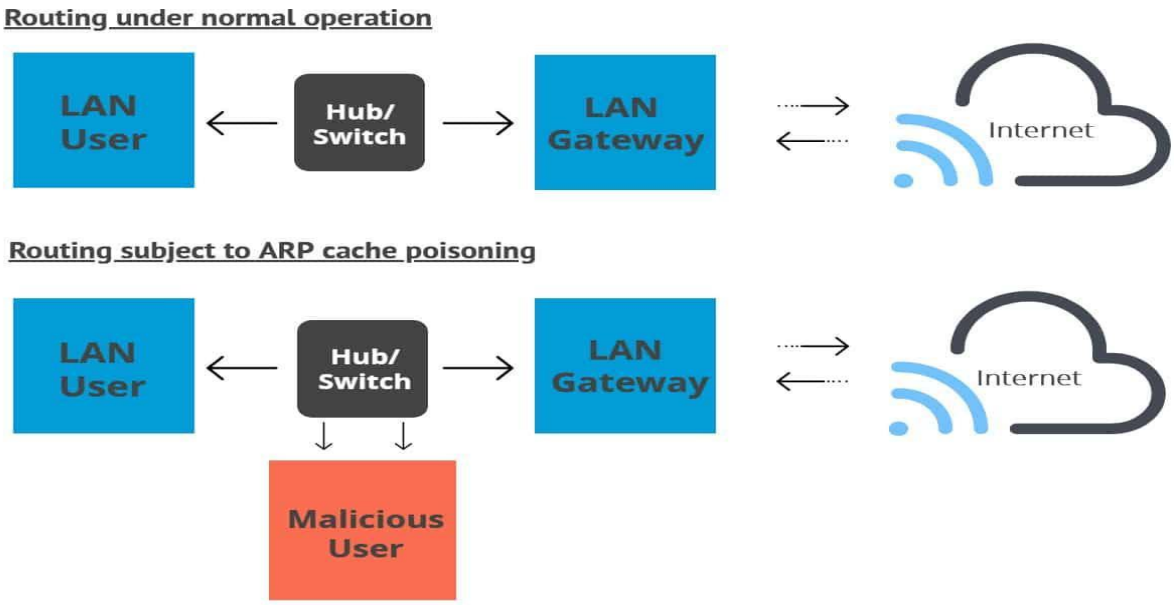
There are two ways that IP spoofing attacks can be used to overload targets with traffic.

One method is to simply flood a selected target with packets from multiple spoofed addresses. This method works by directly sending a victim more data than it can handle.

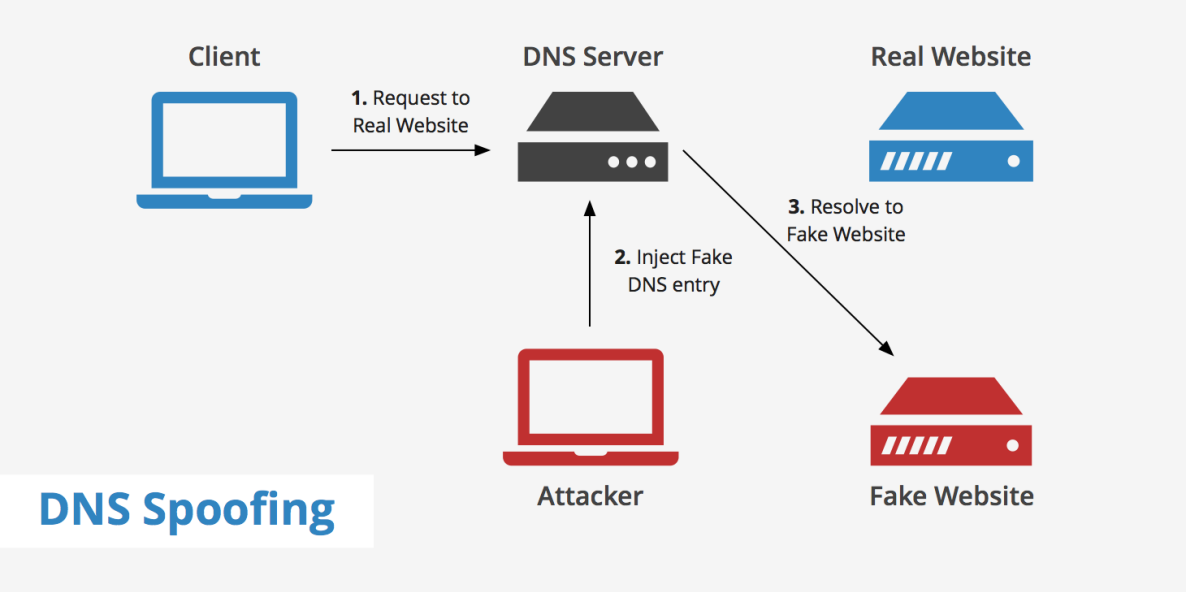
The other method is to spoof the target's IP address and send packets from that address to many different recipients on the network. When another machine receives a packet, it will automatically transmit a packet to the sender in response. Since the spoofed packets appear to be sent from the target's IP address, all responses to the spoofed packets will be sent to (and flood) the target's IP address.

ARP Spoofing Attacks: ARP is short for Address Resolution Protocol, a protocol that is used to resolve IP addresses to MAC (Media Access Control) addresses for transmitting data. In an ARP spoofing attack, a malicious party sends spoofed ARP messages across a local area network in order to link the attacker's MAC address with the IP address of a legitimate member of the network. This type of spoofing attack results in data that is intended for the host's IP address getting sent to the attacker instead. Malicious parties commonly use ARP spoofing to steal information, modify data-in-transit or stop traffic on a LAN. ARP spoofing attacks can also be used to facilitate other types of attacks, including denial-of-service, session hijacking and

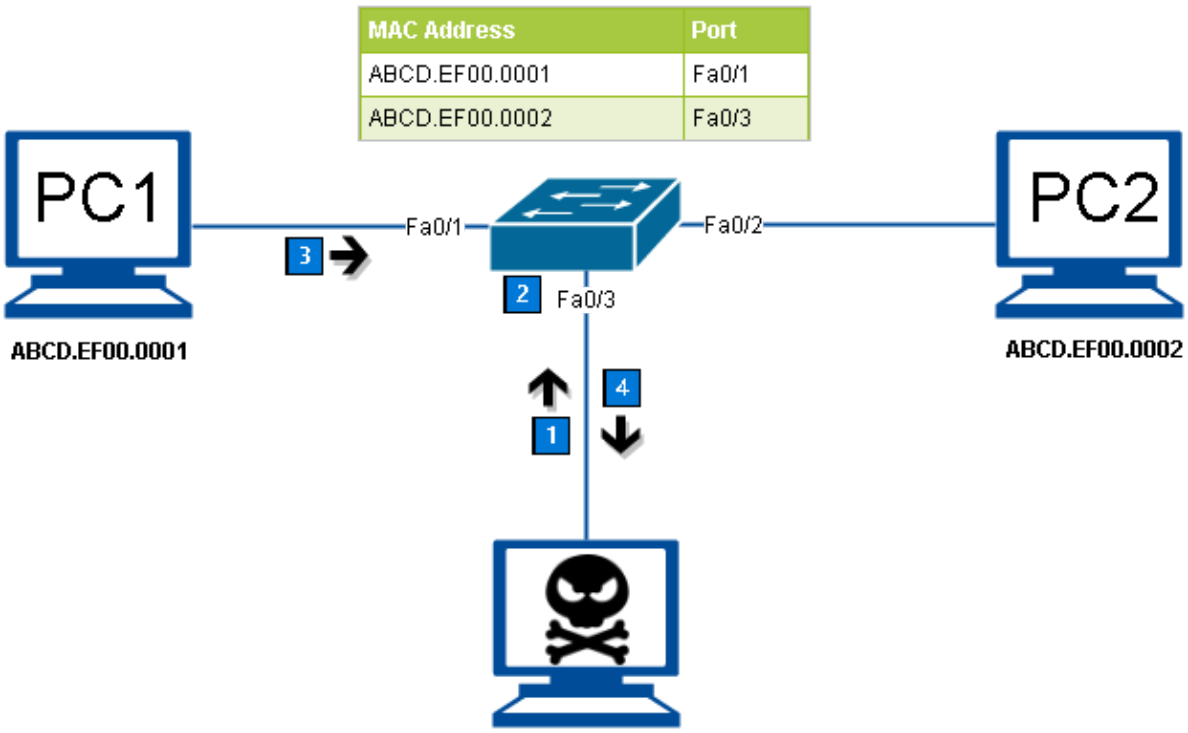
man-in-the-middle attacks. ARP spoofing only works on local area networks that use the Address Resolution Protocol.



DNS Server Spoofing Attacks: The Domain Name System (DNS) is a system that associates domain names with IP addresses. Devices that connect to the internet or other private networks rely on the DNS for resolving URLs, email addresses and other human-readable domain names into their corresponding IP addresses. In a DNS server spoofing attack, a malicious party modifies the DNS server in order to reroute a specific domain name to a different IP address. In many cases, the new IP address will be for a server that is actually controlled by the attacker and contains files infected with malware. DNS server spoofing attacks are often used to spread computer worms and viruses.



MAC Spoofing Attack:MAC spoofing attacks occur when an attacker alters the MAC address of their host to match another known MAC address of a target host. The attacking host then sends a frame throughout the network with the newly configured MAC address. When the switch receives the frame, it examines the source MAC address. The switch overwrites the current MAC address table entry and assigns the MAC address to the new port. It then inadvertently forwards frames destined for the target host to the attacking host.



Port scanning : Port scanning tools are designed to send traffic to remote systems and then gather responses that provide information about the systems and the services they provide. They are one of the most frequently used tools when gathering information about a network and the devices that are connected to it. Due to this, port scans are often the first step in an active reconnaissance of an organization.

Port scanners have a number of common features, including

- ❖ Host discovery
- ❖ Port scanning and service identification
- ❖ Service version identification
- ❖ Operating system identification.

A port is: Endpoint of logical connections

- ❖ Numbered from 0 to 65,535

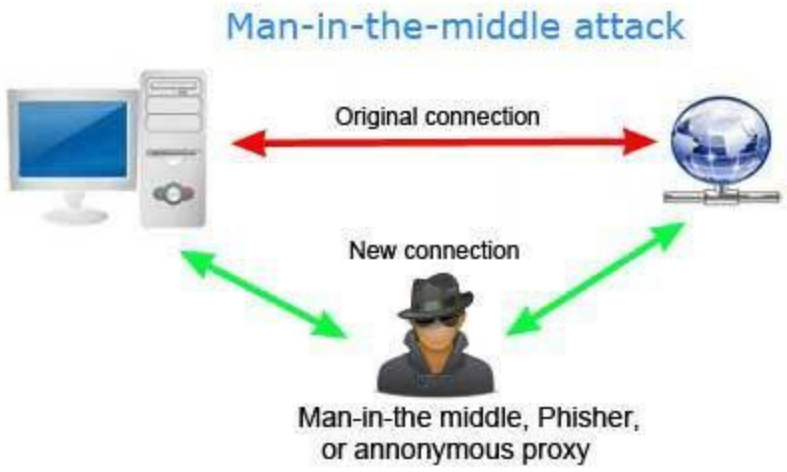
Ports are Divided into three blocks:

- ❖ Well-known ports : 0 – 1023 Specific port numbers most vulnerable to attacks.
- ❖ Registered ports : 1024 – 49151 Too system Specific for direct target by attackers.
- ❖ Dynamic ports : 49152 – 65535 Constantly changing and are used by any application to use in communicating with any other application.

** NMAP network mapper is the tool used for Port Scanning **

Eavesdropping Attack : An eavesdropping attack, which are also known as a sniffing or snooping attack, is an incursion where someone tries to steal information that computers, smartphones, or other devices transmit over a network. An eavesdropping attack takes advantage of unsecured network communications in order to access the data being sent and received. Eavesdropping attacks are difficult to detect because they do not cause network transmissions to appear to be operating abnormally.

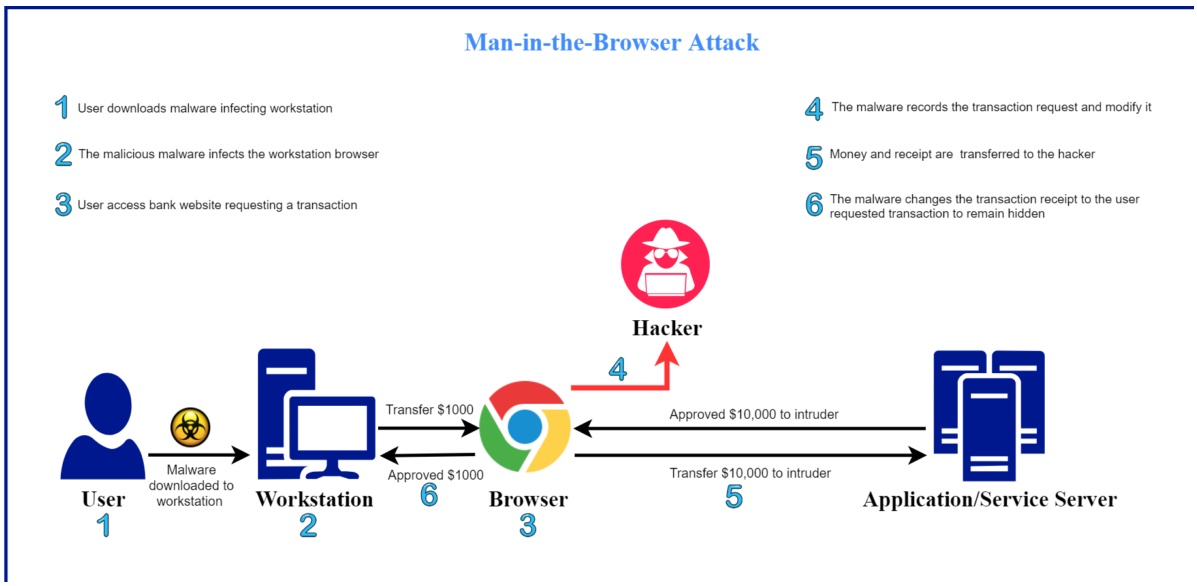
Man-in-the-Middle-Attacks: In cryptography and computer security, a man-in-the-middle attack is an attack where the attacker secretly relays and possibly alters the communications between two parties who believe they are directly communicating with each other.



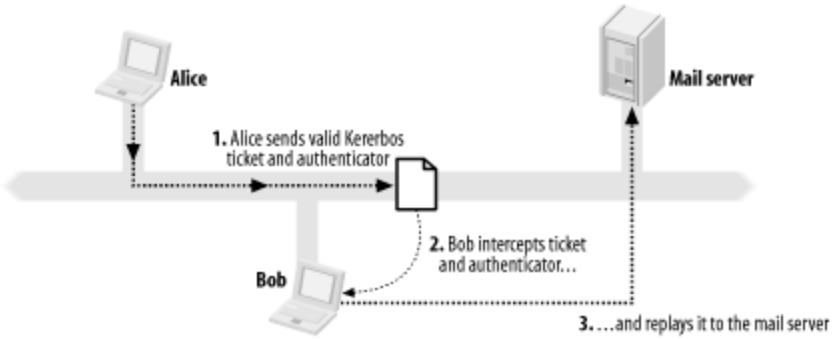
Man-in-the-Browser-Attacks: The man-in-the-browser (MITB) attack utilizes a Trojan Horse in a pre-infected device/system to infect the internet browser, and sniff, capture and modify information as it travels between the user interface of the infected browser and the internet.

MITB malware is a Trojan that infects endpoints through malicious email attachments, links, or even when a user visits an infected website. Cyber criminals target victims through social engineering - phishing and targeted spearphishing attacks to attempt infection. These attacks are constantly evolving and are becoming more sophisticated

and difficult to detect even by experienced cyber security experts.

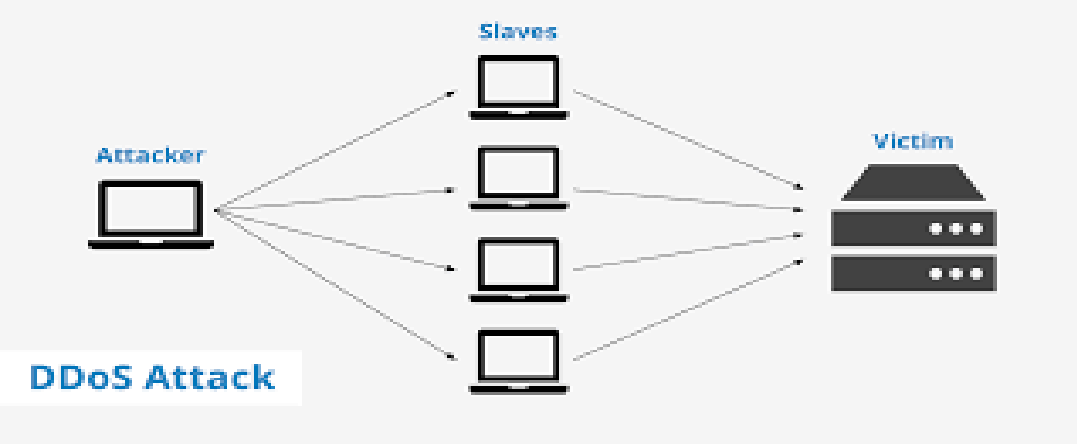


Replay Attacks: A replay attack is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. This is carried out either by the originator or by an adversary who intercepts the data and re-transmits it, possibly as part of a masquerade attack by IP packet substitution.



DOS Attacks : In computing, a denial-of-service attack is a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet.

DDOS attacks : A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic. DDoS attacks achieve effectiveness by utilizing multiple compromised computer systems as sources of attack traffic. Exploited machines can include computers and other networked resources such as IoT devices.



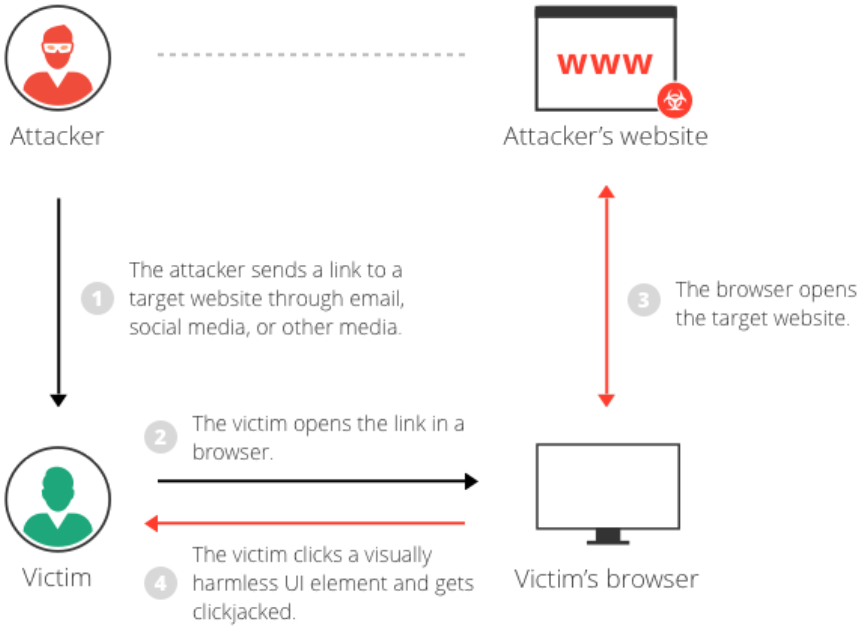
Hijacking Attacks: Hijacking encompasses a group of network based attacks where attacker gains control of the communication between two computers and masquerades as one of them.

Types of Hijacking Attacks Includes the following.

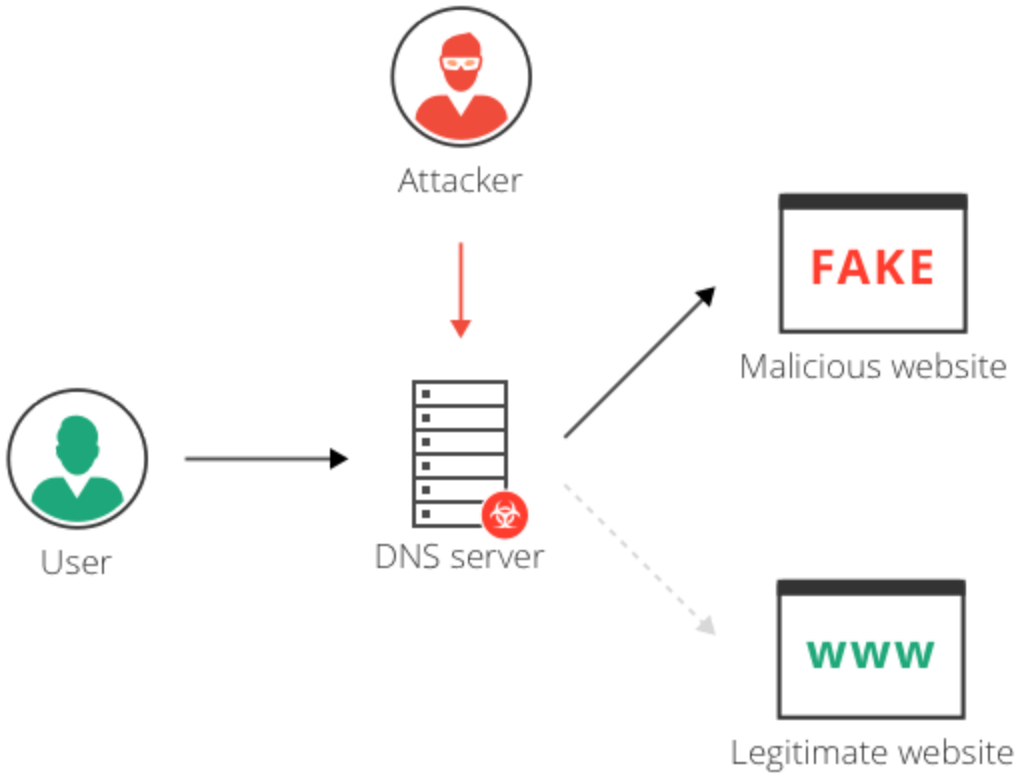
- Click jacking
- DNS hijacking
- Domain hijacking
- Session hijacking
- URL hijacking/Typosquatting

Click jacking: Click jacking is a malicious technique of tricking a user into clicking on something different from what the user perceives, thus potentially revealing confidential information or allowing others to take control of their computer while clicking on seemingly innocuous objects,

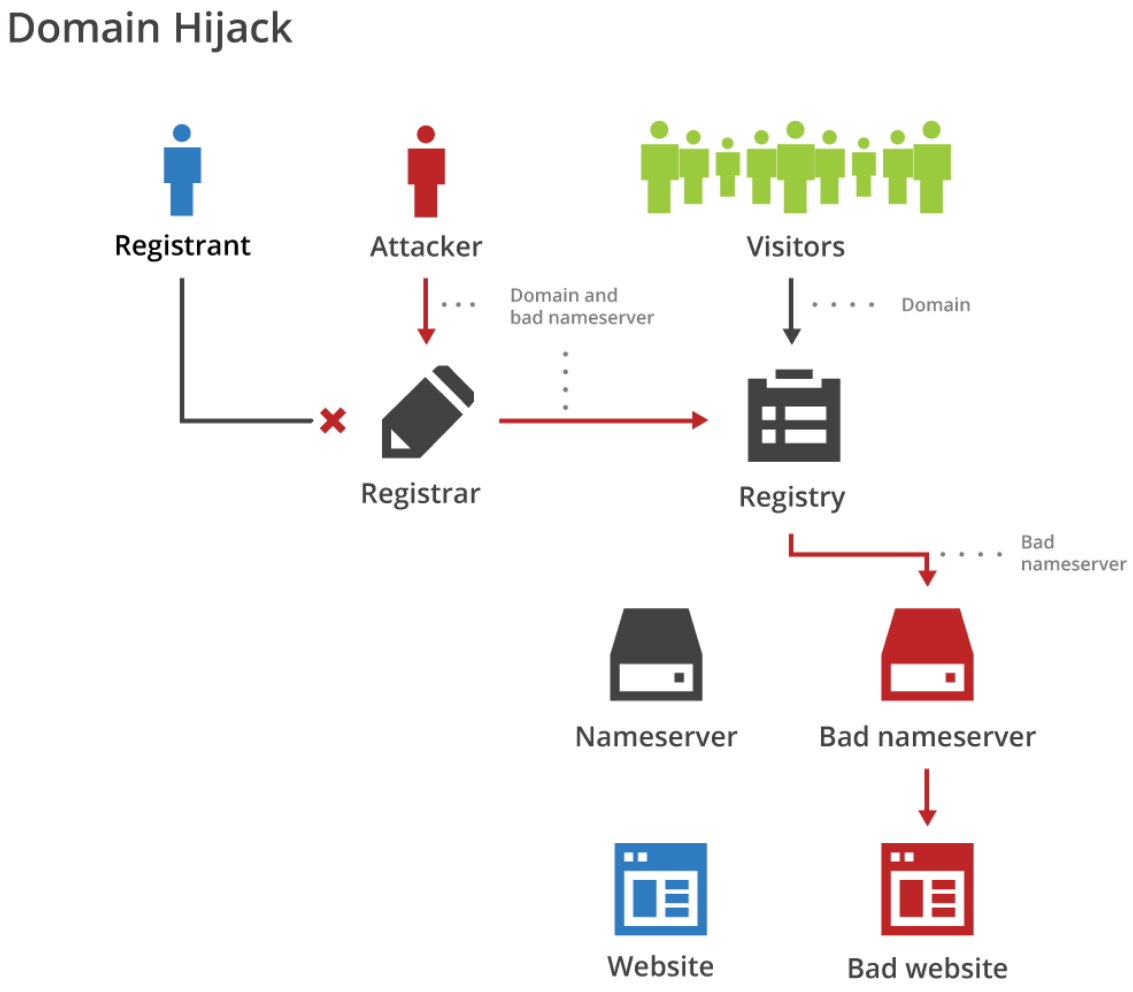
including web pages.



DNS hijacking: The attacker set up a rouge DNS server that responds to legitimate request with IP address from malicious or non-existent website.



Domain Hijacking:The attacker steals a domain name by altering its registration information and then transferring the domain name to another entity sometimes reffered to as brandjacking.

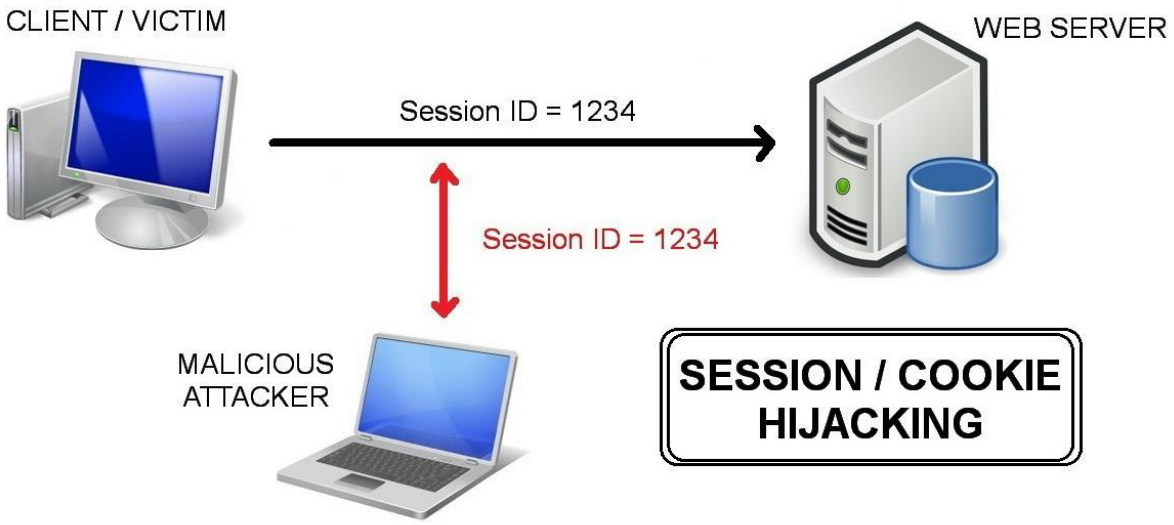


Session hijacking: The Session Hijacking attack consists of the exploitation of the web session control mechanism, which is normally managed for a session token.Because http communication uses many different TCP connections, the web server needs a method to recognize every user's connections. The most useful method depends on a token that the Web Server sends to the client browser after a

successful client authentication. A session token is normally composed of a string of variable width and it could be used in different ways, like in the URL, in the header of the http requisition as a cookie, in other parts of the header of the http request, or yet in the body of the http requisition.The Session Hijacking attack compromises the session token by stealing or predicting a valid session token to gain unauthorized access to the Web Server.

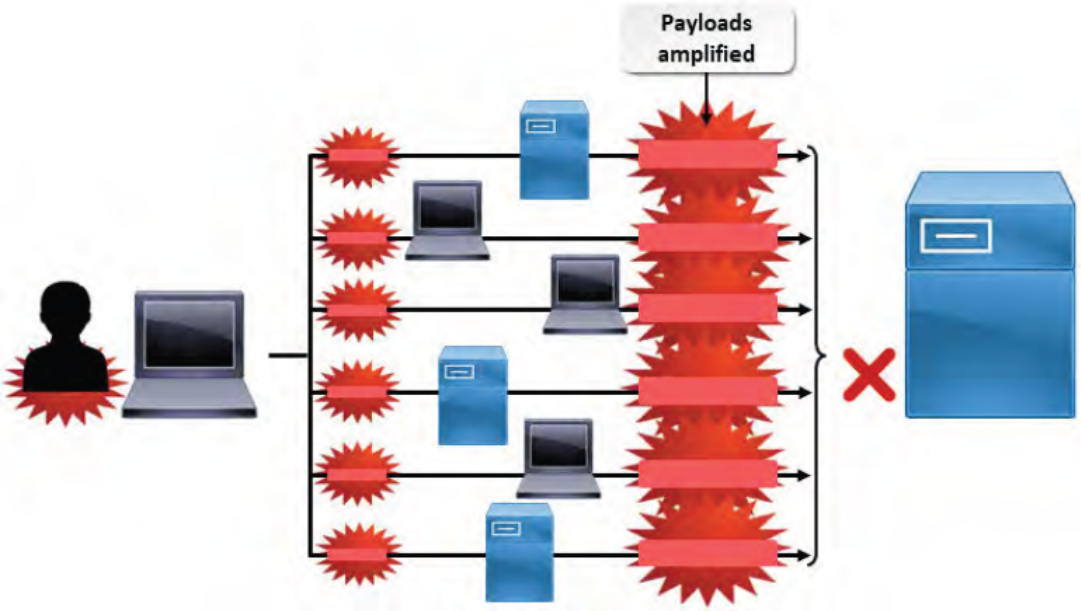
The session token could be compromised in different ways; the most common are:

- Predictable session token;
- Session Sniffing;
- Client-side attacks (XSS, malicious JavaScript Codes,Trojans, etc);
- Man-in-the-middle attack
- Man-in-the-browser attack



URL hijacking/Typosquatting: The attacker registers domain name that closely resembles the names of legitimate websites to take advantage of the possibility of the domain name being mistyped into the browser.

Amplification Attack: An amplification attack is a network based where attacker dramatically increase the bandwidth sent to the victim during a DDOS attack.

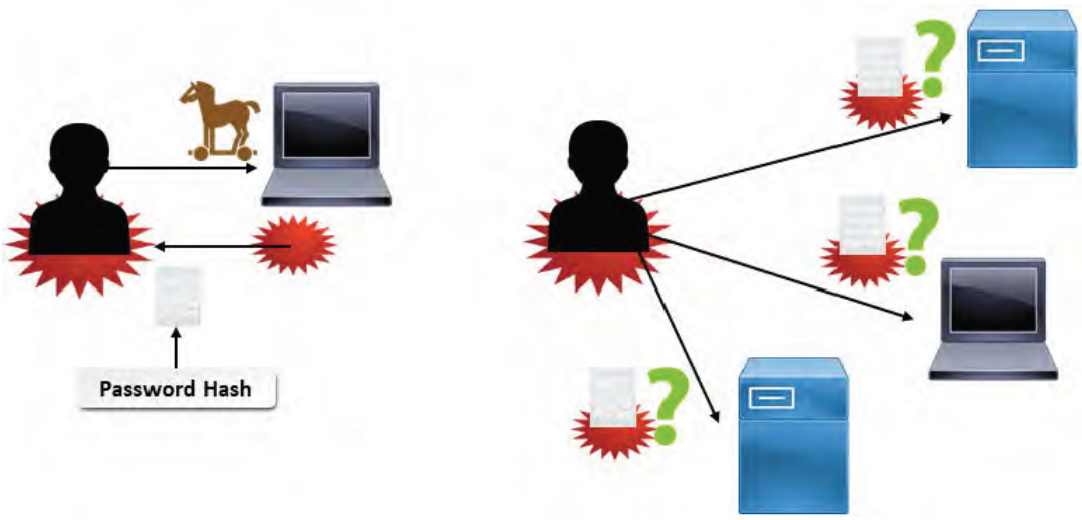


Types of amplification Attack.

- **ICMP amplification:** Most commonly known as smurf attack are based on sending high volumes of ICMP ping packets to a targeted host.
- **DNS amplification:** In this attack the attacker sends DNS query with victims IP address to a DNS server which replies to a spoofed address with a DNS response. If the attacker request additional information about zones, the response packet can be up to 179 times size of a normal DNS packet. When multiple fake queries are sent to different DNS servers, and with several DNS servers replying simultaneously, the victim's network get flooded by sheer number of DNS response.

- **UDP amplification:** It is a type of Denial of Service (DoS) attack in which the attacker overwhelms random ports on the targeted host with IP packets containing UDP datagram's. The receiving host checks for applications associated with these datagram's and finding none sends back a Destination Unreachable packet. As more and more UDP packets are received and answered, the system becomes overwhelmed and unresponsive to other clients.
- **NTP amplification:** NTP amplification is a type of Distributed Denial of Service (DDoS) attack in which the attacker exploits publically-accessible Network Time Protocol (NTP) servers to overwhelm the targeted with User Datagram Protocol (UDP) traffic.

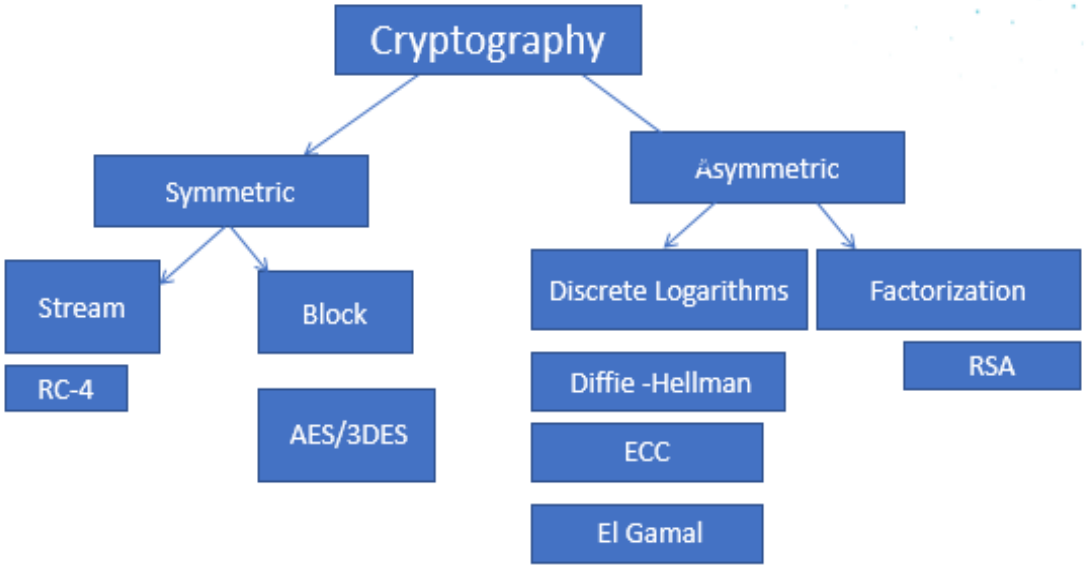
Pass the Hash Attack: In cryptanalysis and computer security, pass the hash is a hacking technique that allows an attacker to authenticate to a remote server or service by using the underlying NTLM or LanMan hash of a user's password, instead of requiring the associated plaintext password as is normally the case.



Pass the Hash Attack

Chapter 6: Cryptography

Cryptography : Cryptography is associated with the process of converting ordinary plain text into unintelligible text and vice-versa. It is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. Cryptography not only protects data from theft or alteration, but can also be used for user authentication.



Security Services provided by Cryptography

- ❖ Privacy: Prevents unauthorized disclosure of information
- ❖ Authenticity: Verifies the claimed identity
- ❖ Integrity: Detects modification or corruption

- ❖ Non-Repudiation: Combines authenticity and integrity. A sender can't dispute having sent a message, nor its contents.

Definitions and Concepts

Plain Text + Initialization Vector + Algorithm (aka Cipher) + Key = Cipher Text

- Plain text is unencrypted text
- Initialization Vector (IV) adds randomness to the beginning of the process
- Algorithm is the collection of math functions that can be performed
- Key: Instruction set on how to use the algorithm

Elements of Cryptography

Desirable Qualities of an Algorithm

- ❖ Confusion
- ❖ Diffusion
- ❖ Avalanche
- ❖ Permutations
- ❖ Open—Kerchhoff's Principle

Desirable Qualities of a Key

- ❖ Long
- ❖ Random
- ❖ Secret

Symmetric Cryptography:

Symmetric = Same

- In symmetric cryptography the same key is used to both encrypt and decrypt
- Very fast means of encrypting/decrypting with good strength for privacy
- Preferred means of protecting privacy data

Common Symmetric Algorithm

- DES
- 3DES
- AES
- RC-4
- RC-5
- Two Fish

Drawbacks to Symmetric Cryptography

Attributes	Symmetric	Asymmetric
Keys	One key is shared between two or more entities	Each user is granted a "Key Pair" consisting of one public and one private
Key Exchange	Out-of-band	Receiver's Public Key is used to encrypt symmetric session keys
Speed	Algorithm is less complex and faster	Algorithm is more complex and slower
Number of Keys	$\frac{N*(N-1)}{2}$	2N
Use	Bulk encryption, which means encrypting files and communication paths	Key encryption and distributing keys
Security Service Provided	Confidentiality	Confidentiality, authentication, and non-repudiation

Asymmetric Cryptography: Every user has a key pair.

- Public key is made available to anyone who requests it
- Private key is only available to that user and must not be disclosed or shared
- The keys are mathematically related so that anything encrypted with one key can only be decrypted by the other.

Common Asymmetric Algorithms

- DSA
- RSA
- ECC (Elliptical Curve Cryptography)
- El Gamal
- Diffie Hellman
- Knapsack

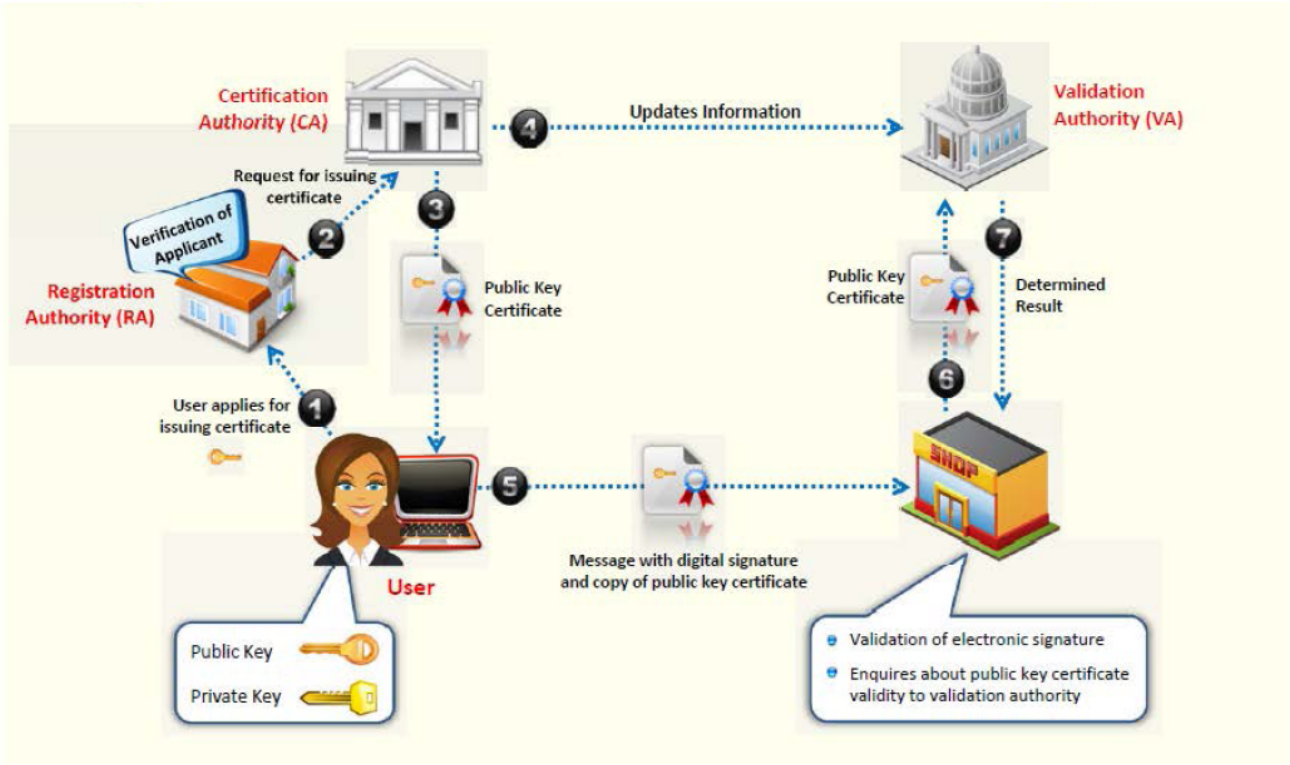
P.A.I.N Services through Asymmetric Cryptography and Hashing

- Privacy: Receiver's Public Key
- Authenticity: Sender's Private Key
- Integrity (not asymmetric OR symmetric)
- Non-Repudiation: Hash encrypted Sender's Private Key

Summary of Symmetric vs. Asymmetric

Attributes	Symmetric	Asymmetric
Keys	One key is shared between two or more entities	One entity has a public key, and the other entity has a private key
Key Exchange	Out-of-band	Public Key is freely shared
Speed	Algorithm is less complex and faster	Algorithm is more complex and slower
Number of Keys	Grows as users grow	Does not grow exponentially
Use	Bulk encryption, which means encrypting files and communication paths	Key encryption and distributing keys
Security Service Provided	Confidentiality	Confidentiality, authentication, and non-repudiation

PKI (Public Key Infrastructure): A public key infrastructure (PKI) is a set of roles, policies, and procedures needed to create, manage, distribute, use, store & revoke digital certificates and manage public-key encryption.



Components of PKI

Certificate Authority (CA): A certificate authority (CA) is an organization that is responsible for issuing, revoking, and distributing certificates. A certificate is nothing more than a mechanism that associates the public key with an individual. It contains a great deal of information about the user. Each user of a PKI system has a certificate that can be used to verify their authenticity.

Registration Authority (RA): A registration authority (RA) offloads some of the work from a CA. An RA system operates as a middleman in the process: It can distribute keys, accept registrations for the CA, and validate identities. The RA doesn't issue certificates; that responsibility remains with the CA.

- **Certificate Repository**: A repository is simply a database or database server where the certificates are stored.
- **Certificate Revocation List** : Certificate revocation is the process of revoking a certificate before it expires. A certificate may need to be revoked because it was stolen, an employee moved to a new company, or someone has had their access revoked. A certificate revocation is handled either through a Certificate Revocation List (CRL) or by using the Online Certificate Status Protocol (OCSP).

Attacks on Cryptography

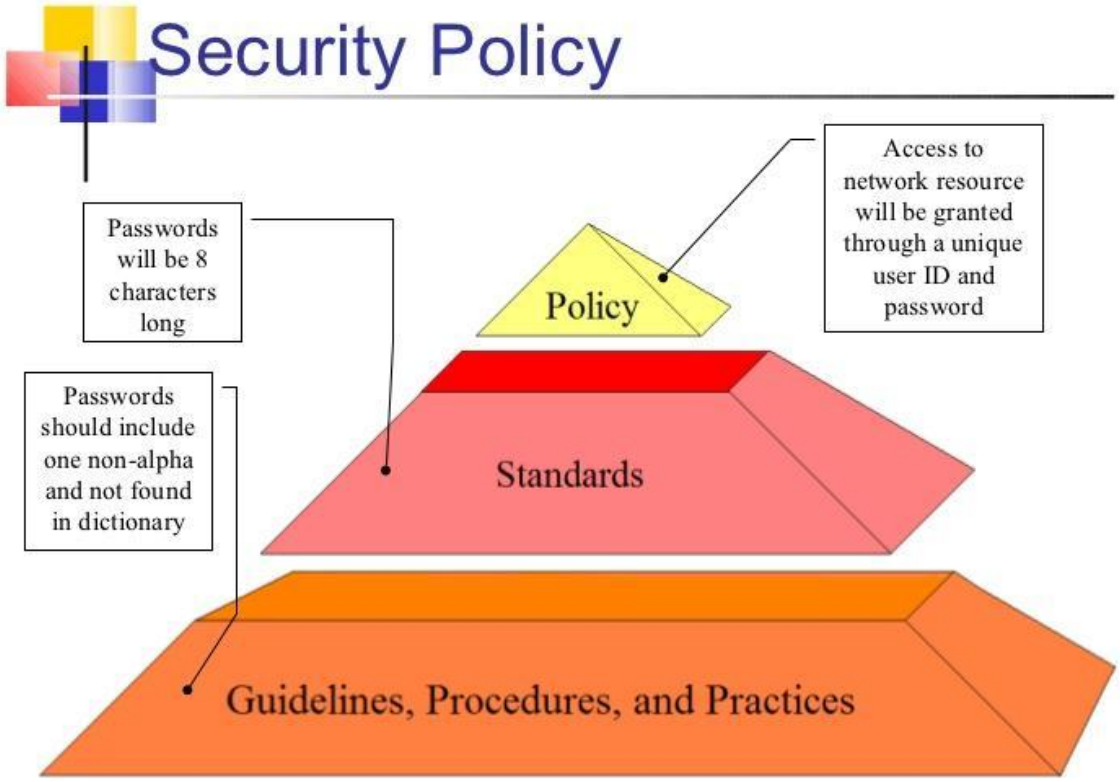
- Known Ciphertext : Attacker has captured encrypted text on the network. Usually means all the attacker can do is brute force
- Known Plain Text: The attacker has captured cipher text, but also knows what a portion of the message is in plain text (like an automatic signature)
- Chosen Plaintext: Attacker can see the full text encrypted and decrypted. Usually the attacker has initiated the message
- Chosen Ciphertext: An attacker can see whatever they want in plain or ciphertext. They have compromised a workstation. Sometimes called a lunchtime or midnight attack.

CHAPTER 7 : Cyber Security Policies & Employee's Role & Responsibilities

Security policies: Security policies define the configuration of systems and networks, including the installation of software, hardware, and network connections. Security policies also define computer room and data center security as well as how identification and authentication (I&A) occurs. These policies determine how access control, audits, reports, and network connectivity are handled. Encryption and antivirus software are usually covered. Security policies also establish procedures and methods used for password selection, account expiration, failed logon attempts, and related areas.

Security Policy Components

- ❖ Standards: Defines how to measure the level of adherence to the policy
- ❖ Guidelines: Describes the suggestions recommendation or best practices for how to meet the standards.
- ❖ Procedures: Step by Step instruction that details how to implement components of policy.



Common Security Policy Types

- ❖ **Acceptable Use Policy** : Acceptable usage policy or fair use policy, is a set of rules applied by the owner,

creator or administrator of a network, website, or service, that restrict the ways in which the network, website or system may be used and sets guidelines as to how it should be used.

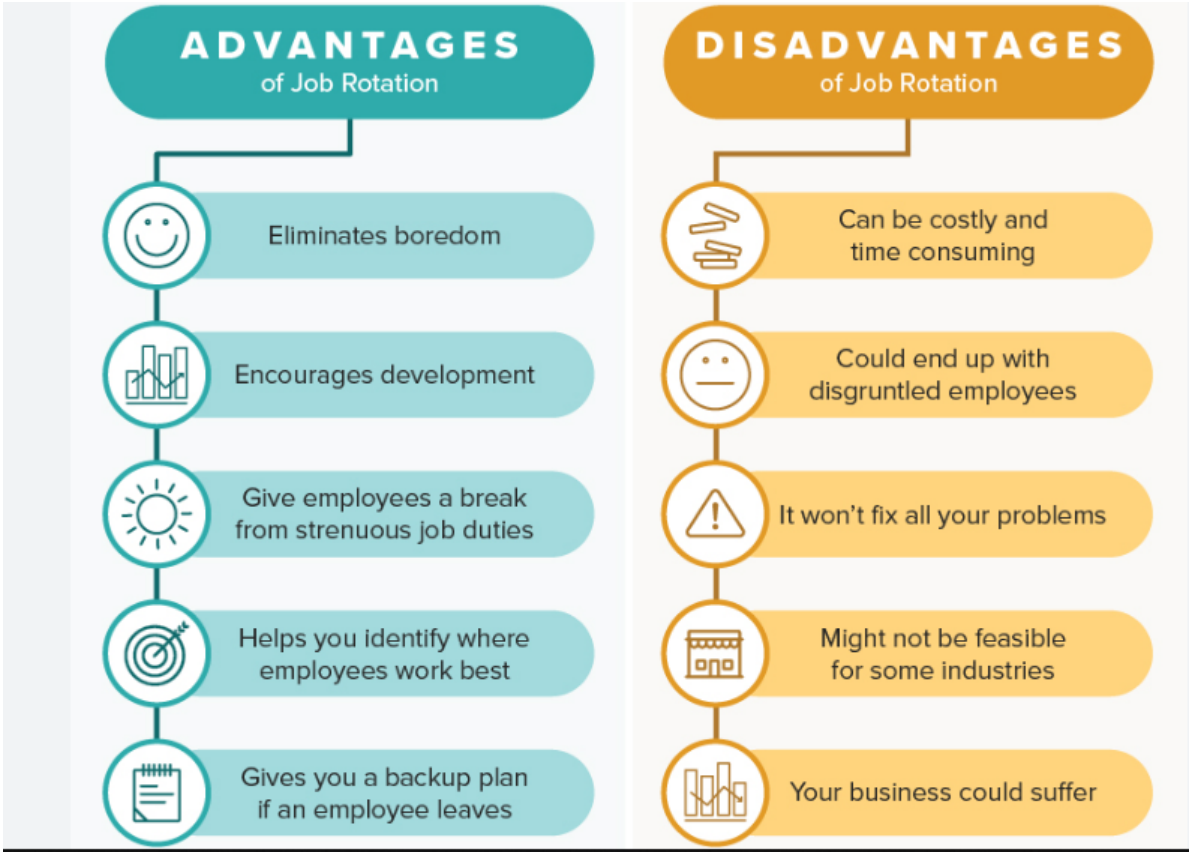
- **Privacy policy :** A privacy policy is a statement or a legal document that discloses some or all of the ways a party gathers, uses, discloses, and manages a customer or client's data. It fulfills a legal requirement to protect a customer or client's privacy.
- **Audit policy:** Details the requirements and parameters for risk assessment and audits of the organization’s information and resources.
- **Password policy:** A password policy is a set of rules designed to enhance computer security by encouraging users to employ strong passwords and use them properly. A password policy is often part of an organization's official regulations and may be taught as part of security awareness training.
- **Wireless standards policy:** Defines which wireless device can connect to organization network and how to use them in a safe manner that protects organizations security.
- **Social media policy:** A social media policy (also called a social networking policy) is a corporate code of conduct that provides guidelines for employees who post content on the Internet either as part of their job or as a private person. The goal of a social media policy is to set expectations for appropriate behavior and ensure that an employee's posts will not expose the

company to legal problems or public embarrassment. Such policies include directives for when an employee should identify himself as a representative of the company on a social networking website, as well as rules for what types of information can be shared. Almost all social media policies include restrictions on disclosing confidential or proprietary business secrets or anything that could influence stock prices.

Personnel Management : It is the practice of ensuring that all of an organization's personal whether internal or external are complying with policies. These includes the following.

Separation of Duties: Separation of duties is the concept of having more than one person required to complete a task. In business the separation by sharing of more than one individual in one single task is an internal control intended to prevent fraud and error.

Job Rotations: Job rotation is a strategy where employees rotate between jobs at the same business. Employees take on new tasks at a different job for a period of time before rotating back to their original position. With a job rotation system, employees gain experience and skills by taking on new responsibilities. Job rotations are meant to promote flexibility, employee engagement, and retention.



Mandatory vacations: Mandatory vacation policies help detect when employees are involved in malicious activity, such as fraud or embezzlement. As an example, employees in positions of fiscal trust, such as stock traders or bank employees, are often required to take an annual vacation of at least five consecutive workdays.

Employee's Role & Responsibilities. Employees play a key role in ensuring the security of your computers and networks, because they are the people using them every day. So it's crucial that they understand their roles and responsibilities in protecting sensitive data and your business resources. Think of

them as the guardians of your data. But for them to be effective, they need to understand what they are protecting, why they are protecting it and how they do it. This means that one of your first steps as a business owner should be to compile a list of policies and procedures around data security to serve as guidelines. Then, you need to train every single employee. While there may be some specialist instances in your business, depending on what data you deal with, most businesses will need to train their employees on at least 5 key things.

Software: A simple thing, but you would be amazed how many employees don't have a clue what they are allowed to download and install onto their work machines. Because downloading software is a process fraught with risk (for businesses in particular), with rogue links and malware downloads always waiting, you need to make sure everyone knows what they are allowed to have and how they should go about it. When in doubt, have them contact your IT department for permission to download a new program, and to have the source checked beforehand.

Password Practices: Work passwords are child's play for the experienced hacker, because so many businesses have 'set' passwords, or they keep the same passwords for long periods of time. Implement a policy that requires all passwords to be changed every 45 to 90 days, and include within that the need for numbers and characters. Educate your employees on the importance of complex passwords in security, and to never

reuse the same password with a different number on the end (something many are guilty of).

Backups: Ensure you have implemented an effective backup system, not only for your main servers, but your employee machines and corporate data as well. Make sure your employees understand that solution, including if they can only recover deleted information for a certain amount of time, to avoid data loss issues. This way if they accidentally delete an important file (it happens more often than you'd think), they know they can just contact IT and recover it, instead of panicking and potentially losing that data forever.

Spam And Phishing Education: One of the biggest methods of infiltration for businesses is through spam or phishing emails. Just one click from a work machine means that the malware can be spread through the entire network, allowing hackers to do as they please. Educate your employees on the issues, including suspicious links and convincing emails. Teach them to hover over links before they click, and to never click on suspicious links in emails, ads or social media posts. Tell them that if they aren't sure, don't click. Make sure you have regular refresher training on this issue.

Ongoing Updates: This flows on quite nicely from the previous point. After your initial training, make sure you keep your employees in the loop about any known issues or scams doing the rounds, to avoid being caught up in them. If you hear of a new phishing email going around (like the Google Doc's one

recently), let people know, and explain how to deal with it if they receive it. Ongoing training and updates helps your employees know what to look for, and how to keep your data safe and secure.

Laws and Regulations governing Cyber security

- **SOX :** In 2002, the United States Congress passed the Sarbanes-Oxley Act (SOX) to protect shareholders and the general public from accounting errors and fraudulent practices in enterprises, and to improve the accuracy of corporate disclosures.
- **HIPPA:** HIPAA (Health Insurance Portability and Accountability Act of 1996) is United States legislation that provides data privacy and security provisions for safeguarding medical information.
- **FISMA:** The Federal Information Security Management Act (FISMA) is United States legislation that defines a comprehensive framework to protect government information, operations and assets against natural or man-made threats. The National Institute of Standards and Technology (NIST) outlines nine steps toward compliance with FISMA:

    - Categorize the information to be protected.
    - Select minimum baseline controls.
    - Refine controls using a risk assessment procedure.
    - Document the controls in the system security plan.

- Implement security controls in appropriate information systems.
- Assess the effectiveness of the security controls once they have been implemented.
- Determine agency-level risk to the mission or business case.
- Authorize the information system for processing.
- Monitor the security controls on a continuous basis.

❖ **GLBA :** The Gramm-Leach-Bliley Act (GLB Act or GLBA) is also known as the Financial Modernization Act of 1999. It is a United States federal law that requires financial institutions to explain how they share and protect their customers' private information.

❖ **PCI-DSS:** The Payment Card Industry Data Security Standard is an information security standard for organizations that handle branded credit cards from the major card schemes. The PCI Standard is mandated by the card brands and administered by the Payment Card Industry Security Standards Council.

❖ **GDPR:** The General Data Protection Regulation is a regulation in EU law on data protection and privacy for all individual citizens of the European Union and the European Economic Area. It also addresses the export of personal data outside the EU and EEA areas.

Data Protection Act: The Data Protection Act 1998 is a United Kingdom Act of Parliament designed to protect personal data stored on computers or in an organized paper filing system. It enacted the EU Data Protection Directive 1995's provisions on the protection, processing and movement of data. The Eight DPA Principles includes.

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept for longer than is necessary.
- Processed in line with your rights.
- Secure.
- Not transferred to other countries without adequate protection

Chapter 8 : Social Engineering

Social engineering: An art of convincing people to reveal their confidential information**.**
An attacker uses human interaction (social skills) to obtain or compromise information about an organization or its computer systems.
Common Targets includes:
Help Desk, Receptionist, Administrator, Technical support executives.

Basic Components of Social Engineering Attacks

- Target Evaluation: In many cases, attackers with specific targets in mind will evaluate those targets & determine how susceptible they to specific type of social engineering. They will also evaluate their general level of awareness of computing technology and cyber security.
- Pre-texting: Attacker will communicate directly or indirectly, a lie, half truth or sin of omission in order to get someone believes a falsehood. This belief may spur victim into committing actions they had not intended.
- Psychological Manipulation: Attackers exploits human willingness to place trust in others.
- Building Relationships: The more friendly & comfortable a victim is with the attacker the more

he will believe the attacker so Attacker will try to know their victim on a personal level. As

- ❖ Motivation: Attacker will motivate the victim to take some actions that will ultimately benefit the attacker.

Motivation Techniques

- ❖ Authority: Focuses on making the target believe that you have the power or right to ask them to perform actions or provide information.
- ❖ Urgency: is the sense that the action needs to be performed, often because of one of the other reasons listed here.
- ❖ Scarcity: It is related to fear-based approaches but focuses on there being fewer rewards or opportunities, requiring faster action and thus creating a sense of urgency.
- ❖ Social Proof: relies on persuading the target that other people have behaved similarly and, thus, that they should or could as well.
- ❖ Likeness: similarity between the social engineer and the target is a means of building trust, as the target is set up to sympathize with the pen-tester due to their similarity.

- Fear: Fear that something will go wrong or that they will be punished if they do not respond or help is a common target.

Phishing Attacks: Phishing attacks target sensitive information like passwords, usernames, or credit card information. While most phishing is done via email, there are many related attacks that can be categorized as types of phishing:

- **Smishing :**uses text messaging to convince victims to disclose account credentials or to install malware..
- **Vishing :** is a form of phishing that occurs over voice communications media, including voice over IP (VoIP) or POTS (plain old telephone service). A typical vishing scam uses speech synthesis software to leave voicemails purporting to notify the victim of suspicious activity in a bank or credit account, and solicits the victim to respond to a malicious phone number to verify his identity thus compromising the victim's account credentials.

- **Whaling :** are a type of spear phishing attack that specifically targets senior executives within an

organization, often with the objective of stealing large sums.

- **Spear phishing :**Are directed at specific individuals or companies, usually using information specific to the victim that has been gathered to more successfully represent the message as being authentic. Spear phishing emails might include references to coworkers or executives at the victim's organization, as well as the use of the victim's name, location or other personal information.
- **Pharming:** It is a type of phishing that depends on DNS cache poisoning to redirect users from a legitimate site to a fraudulent one, and tricking users into using their login credentials to attempt to log in to the fraudulent site.

Impersonation: Impersonation involves disguising yourself as another person to gain access to facilities or resources. This may be as simple as claiming to be a staff member or as complex as wearing a uniform and presenting a false or cloned company ID. Impersonating a technical support worker, maintenance employee, delivery person, or administrative assistant is also common. Impersonation frequently involves pre texting, a technique where the social engineer claims to need information about the person they

are talking to, thus gathering information about the individual so that they can better impersonate them.

Elicitation: It is the practice of researching and discovering the requirements of a system from users, customers, and other stakeholders. The practice is also sometimes referred to as "requirement gathering".

Baiting: Baiting involves offering something enticing to an end user, in exchange for login information or private data. The “bait” comes in many forms, both digital, such as a music or movie download on a peer-to-peer site, and physical, such as a corporate branded flash drive labeled “Executive Salary Summary Q3 2019” that is left out on a desk for an end user to find. Once the bait is downloaded or used, malicious software is delivered directly into the end users system and the hacker is able to get to work.

URL Hijacking/Typo squatting: The attacker registers domain name that closely resembles the names of legitimate websites to take advantage of the possibility of the domain name being mistyped into the browser.

Spam: Spam is an attack where user’s inbox is flooded with unsolicited messages

Spim: Spam carried over instant messaging is called spim.

Piggybacking: When an authorized person allows an unauthorized person inside the secure area

Tailgating: Tailgating is an attack where the attacker slips in through a secure area while following a authorized employee. The employee doesn't know that anyone is behind him.

Shoulder Surfing: Simply watching over a target's shoulder can provide valuable information like passwords or access codes. This is known as shoulder surfing, and high-resolution cameras with zoom lenses can make it possible from long distances.